Oracle® Fusion Middleware

Enterprise Deployment Guide for Oracle WebCenter Content

11*g* Release 1 (11.1.1)

E15483-14

August 2015

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.

ORACLE®

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

E15483-14

Contents

3 Preparing the Network for an Enterprise Deployment

4 Preparing the File System for an Enterprise Deployment

5 Preparing the Database for an Enterprise Deployment

6 Preparing the Servers for an Enterprise Deployment

7 Installing the Software for an Enterprise Deployment

8 Creating a Domain for an Enterprise Deployment

9   Configuring Oracle Web Tier for an Enterprise Deployment

10   Extending the Domain to Include WebCenter Content

11 Extending the Domain to Include Inbound Refinery

12 Extending the Domain to Include Oracle SOA Suite Components

13 Extending the Domain to Include Imaging

15 Installing and Configuring the WebCenter Content User Interface

16 Setting Up Node Manager for an Enterprise Deployment

17 Configuring Server Migration for an Enterprise Deployment

18 Integrating with Oracle Identity Management

19   Managing the Topology for an Enterprise Deployment

A   Using Multi Data Sources with Oracle RAC

B   Targeting Applications and Resources to Servers

Index

List of Figures

List of Tables

Preface

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

Related Documents

This guide refers to the following Oracle Fusion Middleware documents for more information:

- *Administering Oracle WebCenter Enterprise Capture*

- *Administering Oracle WebCenter Content*

- *Oracle Fusion Middleware Administering Oracle WebCenter Content: Imaging*

- *Administrator's Guide*

- *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service*

- *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*

- *Securing Applications with Oracle Platform Security Services*

- *Oracle Fusion Middleware Configuring and Managing JDBC Data Sources for Oracle WebLogic Server*

- *Oracle Fusion Middleware Configuring Server Environments for Oracle WebLogic Server*

- *Oracle Fusion Middleware Developing Oracle WebCenter Content: Imaging*

- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*

- *Oracle Fusion Middleware High Availability Guide*

- *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*

- *Oracle Fusion Middleware Installation Guide for Oracle WebLogic Server*

- *Oracle Fusion Middleware Installation Planning Guide*

- *Installing and Configuring Oracle WebCenter Content*

- *Oracle Fusion Middleware Managing Oracle WebCenter Content*

- *Oracle Fusion Middleware Reference for Oracle Identity Management*

- *Oracle Fusion Middleware Repository Creation Utility User's Guide*

- *Oracle Fusion Middleware User's Guide for Technology Adapters*

- *Oracle Fusion Middleware Using Oracle WebCenter Content*

- *Oracle Fusion Middleware Using Web Server Plug-Ins with Oracle WebLogic Server Guide*

This guide also refers to the following documents for more information:

- *Oracle Coherence Developer's Guide*

- *Oracle Database Administrator's Guide*

- *Oracle Database Backup and Recovery User's Guide*

- *Oracle Fusion Middleware Understanding Domain Configuration for Oracle WebLogic Server*

- *Oracle Grid Infrastructure Installation Guide*

- *Oracle Real Application Clusters Administration and Deployment Guide*

- *Oracle Real Application Clusters Installation Guide for Linux and UNIX*

- *Oracle Universal Installer and OPatch User's Guide*

Conventions

The following text conventions are used in this document.

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

New and Changed Features in This Guide

The following topics introduce the new and changed features of Oracle WebCenter Content and other significant changes that are described in this guide, with cross-references to additional information.

New and Changed Features for Release 11g (11.1.1.9)

This section describes the following new and changed features for Oracle WebCenter Content 11*g* (11.1.1.9):

- Information about how to set up the WebCenter Content user interface, in addition to the native 11*g* user interface, was added. This interface, for Oracle WebCenter Content Server, is based on the Oracle Application Development Framework (Oracle ADF). See Chapter 15, "Installing and Configuring the WebCenter Content User Interface."

- The preferred type of security store for security artifacts, including policies and credentials, is now Oracle Platform Security Services (OPSS) in Oracle Database 11*g* Release 2 (11.2.0.1 or later), rather than Oracle Internet Directory. You can use Oracle Internet directory or another Lightweight Directory Application Protocol (LDAP) provider instead. See Chapter 8, "Creating a Domain for an Enterprise Deployment."

- Oracle WebCenter Capture was rebranded to Oracle WebCenter Enterprise Capture.

New and Changed Features for Release 11g (11.1.1.8)

This section describes the following new and changed features for Oracle WebCenter Content 11*g* (11.1.1.8):

- Oracle WebCenter Enterprise Capture, which provides scalable document capture for centralized or distributed enterprises, extending the Oracle WebCenter Content domain with a new Managed Server

  For Capture information, see these sections:

  - Section 2.2, "About Oracle WebCenter Content"

  - Section 3.4, "IP Addresses and Virtual IP Addresses"

  - Section 4.5, "Shared Storage Configuration"

  - Section 5.4, "Creating Database Schemas"

  - Section 7.3.4.1, "Installing Oracle WebCenter Content"

- Section 10.7, "Configuring Node Manager for the WLS_WCC Managed Servers"

- Chapter 14, "Extending the Domain to Include Capture"

- Section 17.6, "Configuring Server Migration Targets"

- Section 18.4, "Validating Access Through the Load Balancer and SSO"

- Section 19.6.3, "Scale-Up Procedure for Oracle WebCenter Enterprise Capture"

- Section 19.7.3, "Scale-Out Procedure for Oracle WebCenter Enterprise Capture"

- Section 19.9, "Performing Backups and Recoveries in Oracle WebCenter Content Enterprise Deployments."

- Section 11.5.4.2, "Enabling Components for Inbound Refinery on Content Server"

- Section B.5, "Applications and Resources for the Capture Managed Servers"

■ Administration Server interface changes in Oracle WebCenter Content Server, in the following sections:

- Section 9.6.3, "Setting the Front-End URL for the Administration Console and Setting Redirection Preferences,"

- Section 10.4.8, "Configuring Service Retries for Oracle WebCenter Content"

- Section 13.5.8, "Enabling the Imaging Feature Set in Oracle WebCenter Content"

Other Significant Changes in This Document for 11*g* Release 1 (11.1.1)

For 11*g* Release 1 (11.1.1), this guide has been reorganized and updated in several ways:

■ The topology has changed to eliminate the SOAHOST1 and SOAHOST2 hosts. The Oracle SOA Suite Managed Servers are installed and configured on the same two host machines as other managed servers, WCCHOST1 and WCCHOST2. See Section 1.1, "Overview of the Enterprise Deployment Reference Topology."

■ The order of extending the domain with Managed Servers has changed to focus more on Oracle WebCenter Content. See Section 1.6, "Roadmap for the Reference Topology Installation and Configuration."

■ Reassociating the policy story and identity store with an external LDAP provider has been moved to a new chapter, before any of the domain extensions. See Chapter 8, "Creating a Domain for an Enterprise Deployment."

■ Some chapters have been revised for consistency with Oracle Fusion Middleware enterprise deployment guides for other products. See Chapter 3, "Preparing the Network for an Enterprise Deployment," and Chapter 4, "Preparing the File System for an Enterprise Deployment."

1

Introduction to the Enterprise Deployment Reference Topology

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 the following sections:

- Section 1.1, "Overview of the Enterprise Deployment Reference Topology"
- Section 1.2, "Hardware Requirements for an Enterprise Deployment on a Linux System"
- Section 1.3, "Clock Synchronization"
- Section 1.4, "Software Components to Install"
- Section 1.5, "About an LDAP Authentication Provider As a Policy Store"
- Section 1.6, "Roadmap for the Reference Topology Installation and Configuration"

1.1 Overview of the Enterprise Deployment Reference Topology

The diagram in Figure 1–1 illustrates the enterprise deployment reference topology described in this guide. Use this diagram and the information in the following topics to plan your enterprise deployment topology:

- Section 1.1.1, "Reference Topology Documented in This Guide"
- Section 1.1.2, "About Oracle Identity Management Integration"
- Section 1.1.3, "About Oracle Web Tier Nodes"
- Section 1.1.4, "About the Application Tier"
- Section 1.1.5, "About the Data Tier"
- Section 1.1.6, "About the Unicast Requirement for Communication"

1.1.1 Reference Topology Documented in This Guide

This guide provides configuration instructions for a reference enterprise topology that uses Oracle WebCenter Content and Oracle SOA Suite with Oracle Access Manager, as shown in Figure 1–1.

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

Figure 1–1   Reference Topology for Oracle WebCenter Content
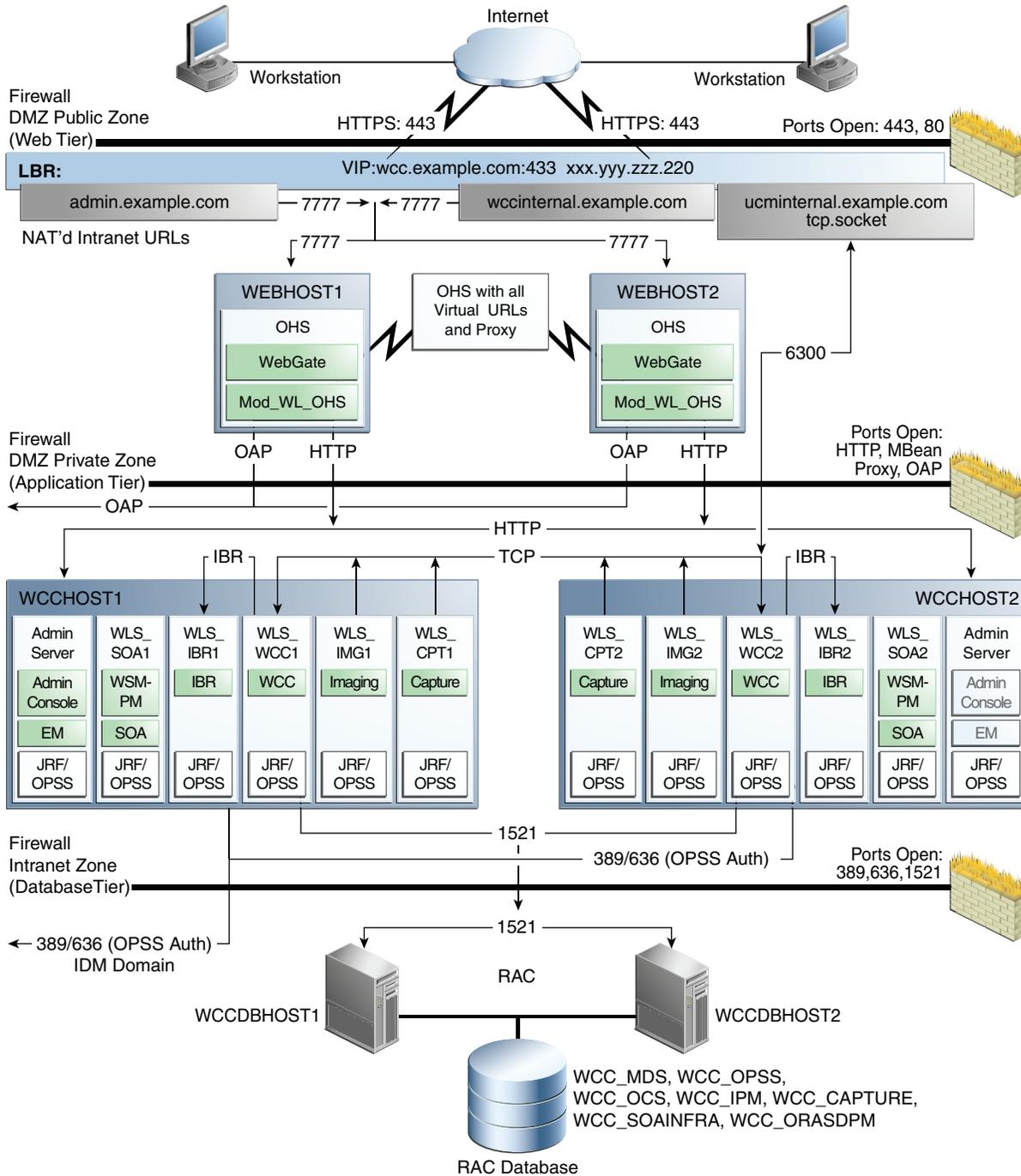
> **Note:** Oracle SOA Suite is required only if your enterprise deployment topology includes Oracle WebCenter Content: Imaging.

The WebCenter Content user interface domain requires its own Middleware home because it uses a newer version of the Oracle Application Development Framework (Oracle ADF) technology stack (11.1.2.4.0). The two Middleware homes and domains can reside on the same host or on different hosts. Figure 1–2 shows the reference topology for the Oracle WebCenter Content user interface.

Figure 1–2   Reference Topology for Oracle WebCenter Content User Interface
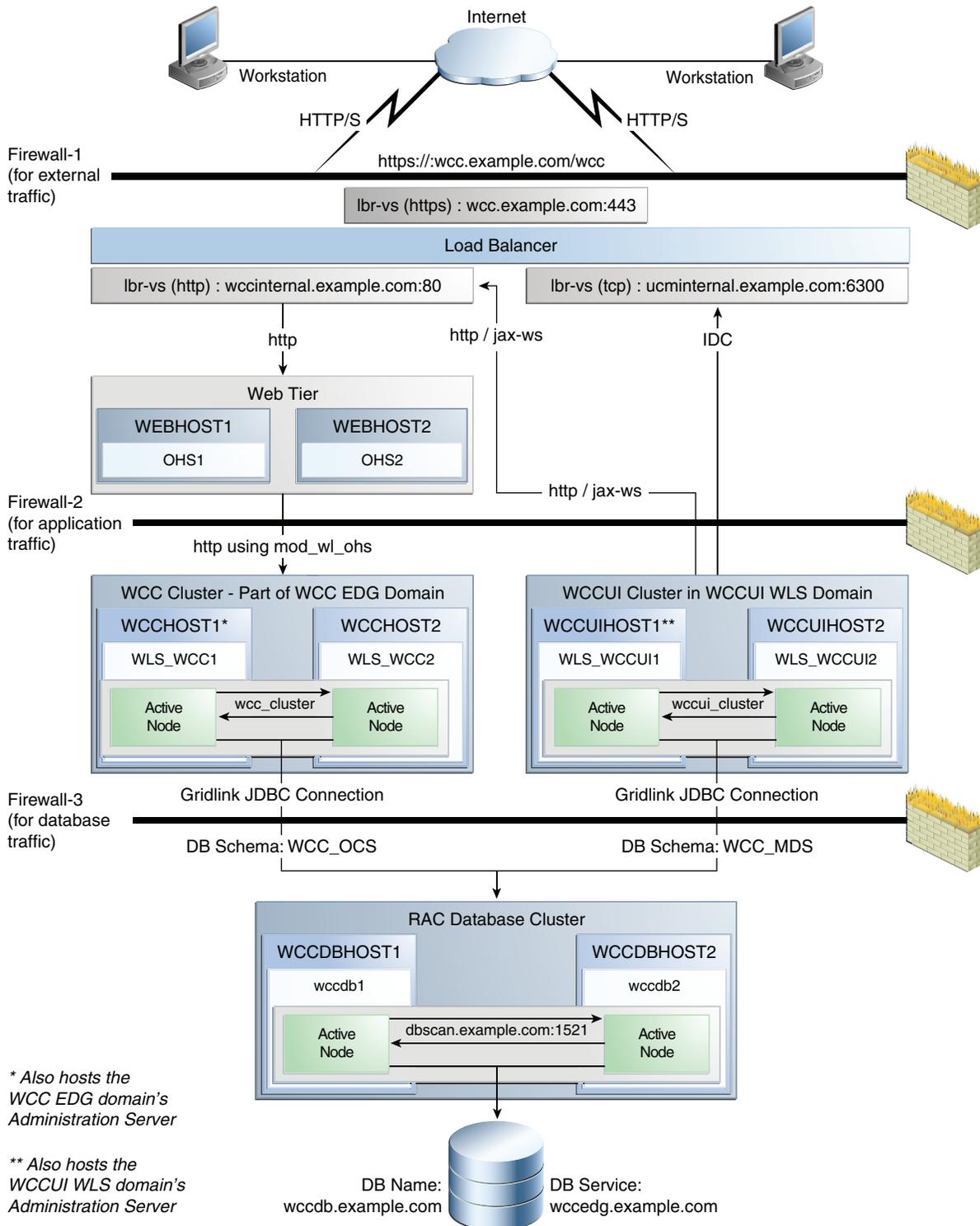
1.1.2 About Oracle Identity Management Integration

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, centralized identity and credential store, and authentication for the Oracle WebLogic Server domain. The Oracle Identity Management 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 Identity Management enterprise deployment is the Lightweight Directory Application Protocol (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.

1.1.3 About Oracle Web Tier Nodes

Nodes in Oracle 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 `*_vh.conf` files.

Through `*_vh.conf` files, which allow 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 (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 Oracle Identity Management DMZ. WebGate and Oracle Access Manager are used to perform operations such as user authentication. 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.

Oracle 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.

On the firewall protecting Oracle 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 Oracle 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.

1.1.4 About the Application Tier

Nodes in the application tier are located in the DMZ secure zone. In this tier, two nodes, WCCHOST1 and WCCHOST2, run Oracle WebLogic Server configured with Managed Servers for running WebCenter Content, Oracle WebCenter Content: Imaging with AXF for BPEL and AXF for BPM, Oracle WebCenter Enterprise Capture, Oracle WebCenter Content: Inbound Refinery, and Oracle SOA Suite components, such as Oracle BPEL Process Manager. The Managed Servers are configured in an active-active manner, except for Inbound Refinery.

WCCHOST1 and WCCHOST2 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 8.6, "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 Oracle 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.)

1.1.5 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 WCCDBHOST1 and WCCDBHOST2. 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 Oracle Identity Management enterprise deployment.

1.1.6 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 to using unicast to handle cluster communications:

- All members of a WebLogic Server 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 Server 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.)

1.2 Hardware Requirements for an Enterprise Deployment on a Linux System

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 1–1 lists the typical hardware requirements for the enterprise deployment described in this guide on a Linux operating system.

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 being used.

Table 1–1   Typical Hardware Requirements

Server	Disk	Memory	TMP Directory	Swap
Database	*nXm* *n* = number of disks, at least 4 (striped as one disk) *m* = size of the disk (minimum of 30 GB)	6-8 GB	Default	Default
WEBHOST*n*	10 GB	4 GB	Default	Default
WCCHOST*n*	20 GB	10 GB	Default	Default

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 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 (JVM) 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 *Installing and Configuring Oracle WebCenter Content*.

1.3 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.

1.4 Software Components to Install

Table 1–2 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 *Oracle Fusion Middleware Download, Installation, and Configuration Readme Files* on the Oracle Technology Network (OTN).

Table 1–2   Components and Installation Sources

Component	Details
Oracle Database 11*g*	Oracle Database 11*g* (11.1.0.7 or later, Standard Edition or Enterprise Edition), using the AL32UTF8 character set
	Note: 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).
Repository Creation Utility (RCU)	Oracle Fusion Middleware Repository Creation Utility 11*g* (11.1.1.9)
Oracle WebLogic Server	Oracle WebLogic Server (10.3.6)
Oracle HTTP Server (OHS)	Oracle Web Tier 11*g* (11.1.1.7)
Oracle WebCenter Content	Oracle WebCenter Content 11*g* (11.1.1.9)
Oracle SOA Suite	Oracle SOA Suite 11*g* (11.1.1.7)
Oracle Access Manager WebGate	WebGate 11*g* (11.1.1.2 or later) for Oracle Access Manager 11*g*.
Oracle Internet Directory	Oracle Identity and Access Management 11*g* (11.1.1.5 or later)

1.5 About an LDAP Authentication Provider As a Policy Store

With Oracle Fusion Middleware, you can use different types of policy and credential stores in an Oracle WebLogic Server domain. Domains can use stores based on XML files, different types of LDAP authentication providers, or Oracle Database. When a domain uses an LDAP store, all policy and credential data is kept and maintained in a centralized policy store. When a domain uses an XML policy store, however, 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 4.4, "Recommended Locations for Different Directories." Derived from this, and for integrity and consistency purposes, Oracle requires the use of an LDAP server as the policy store in the context of an Oracle WebCenter Content enterprise deployment topology. To configure the Oracle WebCenter Content enterprise deployment with an LDAP authentication provider as the policy store, follow the steps in Chapter 8, "Creating a Domain for an Enterprise Deployment."

1.6 Roadmap for the Reference Topology Installation and Configuration

Before beginning your Oracle WebCenter Content enterprise deployment, review the flowchart in Figure 1–3. This flowchart illustrates the high-level process for completing the enterprise deployment documented in this guide. Table 1–3 describes the steps in the flowchart and directs you to the appropriate chapter for each step.

In this document, `oracle` is the operating system user ID for installing and configuring the enterprise deployment reference topology.

The following topics provide a roadmap for installing and configuring the Oracle WebCenter Content reference topology:

- Section 1.6.1, "Flowchart of the Oracle WebCenter Content Enterprise Deployment Process"

- Section 1.6.2, "Steps in the Oracle WebCenter Content Enterprise Deployment Process"

- Section 1.6.3, "The Incremental, Modular Approach to Enterprise Deployment"

1.6.1 Flowchart of the Oracle WebCenter Content Enterprise Deployment Process

Figure 1–3 provides a flowchart 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 1–3   Oracle WebCenter Content Enterprise Deployment Process
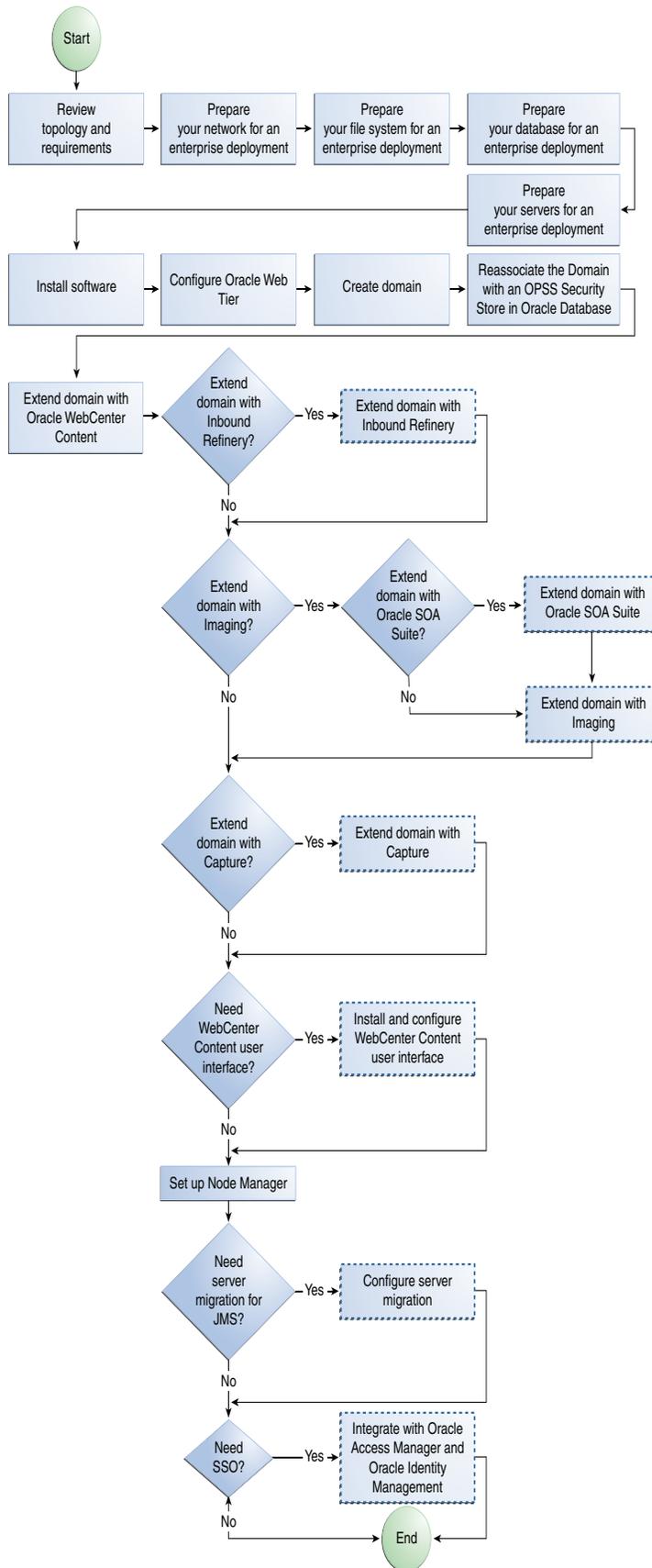
1.6.2 Steps in the Oracle WebCenter Content Enterprise Deployment Process

Table 1–3 describes each of the steps in the enterprise deployment process flowchart for Oracle WebCenter Content, shown in Figure 1–3. The table also provides references to more information on each step in the process.

Table 1–3   Steps in the Oracle WebCenter Content Enterprise Deployment Process

Step	Description	More Information
Review topology and requirements	Read the earlier sections of this chapter for information about the Oracle WebCenter Content enterprise deployment topology and the requirements for setting it up.	Chapter 1, "Introduction to the Enterprise Deployment Reference Topology"
Prepare your network for an enterprise deployment	To prepare your network for an enterprise deployment, understand concepts such as IP addresses, virtual server names, and virtual IP addresses, and configure your load balancer by defining virtual host names.	Chapter 3, "Preparing the Network for an Enterprise Deployment"
Prepare your file system for an enterprise deployment	To prepare your file system for an enterprise deployment, review the terminology for directories and directory environment variables, and configure shared storage.	Chapter 4, "Preparing the File System for an Enterprise Deployment"
Prepare your database for an enterprise deployment	To prepare your database for an enterprise deployment, review database requirements, create database services, load the metadata repository in the Oracle RAC database, configure WebCenter Content, Oracle SOA Suite, Imaging, and Capture schemas for transactional recovery privileges, and back up the database.	Chapter 5, "Preparing the Database for an Enterprise Deployment"
Prepare your servers for an enterprise deployment	To prepare your servers for an enterprise deployment, you need to verify your servers and operating system, meet minimum hardware and operating system requirements, enable Unicode support and virtual IP addresses, mount shared storage onto the host, and configure users and groups.	Chapter 6, "Preparing the Servers for an Enterprise Deployment"
Install software	Install Oracle HTTP Server, Oracle WebLogic Server, and Oracle Fusion Middleware, and apply patchsets to Oracle Fusion Middleware components.	Chapter 7, "Installing the Software for an Enterprise Deployment"
Configure Oracle Web Tier	Configure Oracle HTTP Server with the load balancer, and configure virtual host names.	Chapter 9, "Configuring Oracle Web Tier for an Enterprise Deployment"
Create domain	Run the Fusion Middleware Configuration Wizard to create a domain.	Chapter 8, "Creating a Domain for an Enterprise Deployment"

Table 1–3   (Cont.) Steps in the Oracle WebCenter Content Enterprise Deployment Process

Step	Description	More Information
Reassociate the security store with an OPSS database-based security store	Reassociate the default file-based security store for the domain with an OPSS database-based security store in Oracle Database. The security store contains security artifacts, including policies, credentials, and keys.	Chapter 8.5, "Reassociating the Domain with an OPSS Security Store in Oracle Database"
Extend domain with WebCenter Content	Extend the existing WebLogic Server domain by running the Fusion Middleware Configuration Wizard and configuring WebCenter Content.	Chapter 10, "Extending the Domain to Include WebCenter Content"
Extend domain with IBR (optional)	Extend the existing WebLogic Server domain by running the Fusion Middleware Configuration Wizard and configuring Inbound Refinery.	Section 11, "Extending the Domain to Include Inbound Refinery"
Extend domain with SOA (optional)	Before extending the existing WebLogic Server domain with Imaging, extend the domain by running the Fusion Middleware Configuration Wizard and configuring Oracle SOA Suite.	Chapter 12, "Extending the Domain to Include Oracle SOA Suite Components"
Extend domain with Imaging (optional)	Extend the existing WebLogic Server domain by running the Fusion Middleware Configuration Wizard and configuring Imaging.	Chapter 13, "Extending the Domain to Include Imaging"
Extend domain with Capture (optional)	Extend the existing WebLogic Server domain by running the Fusion Middleware Configuration Wizard and configuring Capture.	Chapter 14, "Extending the Domain to Include Capture"
Set up Node Manager	Set up Node Manager by enabling host name verification, starting Node Manager, and configuring WebLogic Server domains to use custom keystores.	Section 16, "Setting Up Node Manager for an Enterprise Deployment"
Install and Configure the WebCenter Content User Interface (optional)	Install and configure an Oracle WebCenter Content Managed Server with the WebCenter Content user interface for Oracle WebCenter Content Server, based on Oracle ADF.	Section 15, "Installing and Configuring the WebCenter Content User Interface"
Configure Server Migration (optional)	Configure server migration for the WLS_IMGn, WLS_CPTn, and WLS_SOAn Managed Servers. The WLS_IMG1, WLS_CPT1, and WLS_SOA1 Managed Servers are configured to restart on WCCHOST2, should a failure occur. The WLS_IMG2, WLS_CPT2, and WLS_SOA2 Managed Servers are configured to restart on WCCHOST1, should a failure occur.	Section 17, "Configuring Server Migration for an Enterprise Deployment"
Integrate with OAM/IDM (optional)	You can integrate your Oracle WebCenter Content enterprise deployment with Oracle Access Manager 11g for single sign-on (SSO).	Section 18, "Integrating with Oracle Identity Management"

1.6.3 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 Oracle 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 that you later configure to support your 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.

2

Enterprise Deployment Overview

This chapter provides an overview of the enterprise deployment for Oracle WebCenter Content.

This chapter includes the following sections:

2.1 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 this blueprint span 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 provides the following benefits:

- Considers various business service level agreements (SLAs) to make high-availability best practices as widely applicable as possible

- Leverages database grid servers and storage grid with low-cost storage to provide highly resilient, lower-cost infrastructure

- Uses results from extensive performance impact studies for different configurations to ensure that the high-availability architecture is optimally configured to perform and scale to business needs

- Enables control over the length of time to recover from an outage and the amount of acceptable data loss from a natural disaster

- Uses Oracle best practices and recommended architecture, which are independent of hardware and operating systems

For more information about high availability practices, see the Oracle Maximum Availability Architecture Best Practices page on the Oracle Technology Network at http://www.oracle.com/technetwork/database/features/availability/maa-best-practices-155366.html.

> **Note:** This document focuses on enterprise deployments in Linux environments, but enterprise deployments can also be implemented in UNIX and Windows environments.

2.2 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 through the Oracle Application Extension Framework (AXF).

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 auditability, 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: Inbound Refinery

- Oracle WebCenter Content: Imaging

- Oracle WebCenter Enterprise Capture

Oracle WebCenter Content

WebCenter Content (formerly known as Oracle Universal Content Management, or Oracle UCM), which includes Oracle WebCenter Content Server, 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.

You can configure Content Server with the WebCenter Content user interface in addition to the native 11*g* user interface, which Content Server uses by default. For information about the WebCenter Content user interface, see Chapter 15, "Installing and Configuring the WebCenter Content User Interface."

Oracle WebCenter Content: Imaging

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 Forms Recognition for intelligent data capture, AXF for orchestration of LOB and process collaboration, and Oracle WebCenter Enterprise Capture for image capture. It also provides annotation and markup of images, automated routing and approvals, and a scalable repository that supports enterprise-wide applications. With Imaging, organizations can quickly automate business processes in Oracle and third-party enterprise applications.

Oracle WebCenter Content: Inbound Refinery

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.

Oracle WebCenter Enterprise Capture

Capture provides scalable document capture for centralized or distributed enterprises. It is fully integrated with Oracle WebCenter Content: Imaging and Oracle WebCenter Content to provide organizations with one system to capture, store, manage, and retrieve their mission critical business content.

Oracle WebCenter Enterprise Capture provides scanning and optional indexing at remote locations using the Internet or a corporate intranet. When you scan images with Capture, it copies them to your local machine. You can view the images there until you release a batch of them. Then they go to the server. You scan your batches, and then you can organize your documents the way you need to. The documents can be imported into Capture. You can import documents from a scanner, add items from other sources, and then add an index.

2.3 Enterprise Deployment Terminology

The following terminology is used in this enterprise deployment guide:

- **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 through 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.

- **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 prefailure configuration.

- **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. For information about active-active and active-passive system, see the *Oracle Fusion Middleware High Availability Guide*.

- **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 or 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.

- **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.

- **network host name**: A 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 is connected. Often, the network host name and physical host name are identical. However, each machine has only one physical host name but can have multiple network host names. Thus, a machine's network host name may not always be its physical host name.

- **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).

- **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 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.

- **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 a UNIX system, this is the name returned by the `hostname` command.

  A 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 address**: A physical IP address is the IP address of a machine on the network. In most cases, it is associated with the physical host name of the machine (see the definition of the physical host name). In contrast to a virtual IP address, a physical IP address is always associated with the same machine when on a network.

- **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, or 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 scenario based on server migration, 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 the preceding text.

- **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.

- **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.

- **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.

- **virtual host name**: A virtual host name is a network-addressable host name that maps to one or more physical machines through a load balancer or a hardware cluster. For load balancers, the term *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 the cluster's virtual IP address. Because the virtual IP address 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, this will be explicitly stated.

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

  A hardware cluster uses a cluster virtual IP address to present to the outside world as the entry point into the cluster. (A cluster virtual IP address 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 address 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.

- **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.

2.4 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.

The security and high-availability benefits of the Oracle Fusion Middleware configurations are realized through isolation in firewall zones and replication of software components, as these topics describe:

- Section 2.4.1, "Built-In Security"

- Section 2.4.2, "High Availability"

2.4.1 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: Oracle Web Tier, the 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.

2.4.2 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.

3

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, IP addresses, virtual IP addresses, and firewalls and ports.

This chapter includes the following sections:

- 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, "Load Balancers"
- Section 3.4, "IP Addresses and Virtual IP Addresses"
- Section 3.5, "Firewalls and Ports"

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, "admin.example.com"
- Section 3.2.2, "wcc.example.com"
- Section 3.2.3, "wccinternal.example.com"
- Section 3.2.4, "ucminternal.example.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

3.2.1 admin.example.com

The address `admin.example.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.example.com:80`, and the requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2.

3.2.2 wcc.example.com

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

3.2.3 wccinternal.example.com

The address `wccinternal.example.com` is a virtual server name used for internal invocations of SOA and WebCenter Content services. This URL is not exposed to the Internet and is accessible only from the intranet. (For Oracle SOA Suite systems, users can set this URL while modeling composites or at runtime with the appropriate MBean through Fusion Middleware Control, as the URL to be used for invoking internal services.) You can use this URL for any service call back to WebCenter Content components from Oracle SOA Suite.

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

3.2.4 ucminternal.example.com

The address `ucminternal.example.com` is a virtual server name that acts as the access point for all internal Remote Intradoc Client (RIDC) TCP traffic to the runtime Oracle WebCenter Content components. Applications like Imaging and Capture access this service using the address `ucminternal.example.com:6300` for RIDC connections, and the requests are forwarded to port 4444 on WCCHOST1 and WCCHOST2.

Instead of having an additional IP address, you can use `wccinternal.example.com:6300` in lieu of `ucminternal.example.com:6300`. For clarity, the reference topology in this guide shows separate IP addresses.

3.3 Load Balancers

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

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

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."

For more information on load balancers, see Section 1.1.3, "About Oracle Web Tier Nodes."

3.3.1 Understanding Load Balancer Requirements

The enterprise topologies use an external load balancer. This external load balancer must have the following features:

- Ability to load-balance traffic to a pool of real servers through a virtual host name: Clients access services using the virtual host name (instead of using actual host names). The load balancer can then load balance requests to the servers in the pool.

- Port translation configuration.

- Monitoring of ports (HTTP and HTTPS).

- Virtual servers and port configuration: Ability to configure virtual server names and ports on your external load balancer, and the virtual server names and ports must meet the following requirements:

  - The load balancer should allow configuration of multiple virtual servers. For each virtual server, the load balancer should allow configuration of traffic management on more than one port. For example, for Oracle WebLogic Server clusters, the load balancer must be configured with a virtual server and ports for HTTP and HTTPS traffic.

  - The virtual server names must be associated with IP addresses and be part of your DNS. Clients must be able to access the external load balancer through the virtual server names.

- Ability to detect node failures and immediately stop routing traffic to the failed node.

- Resource monitoring, port monitoring, and process failure detection: The load balancer must be able to detect service and node failures (through notification or some other means) and to stop directing non-Oracle Net traffic to the failed node. If your external load balancer has the ability to automatically detect failures, you should use it.

- Fault-tolerant mode: It is highly recommended that you configure the load balancer to be in fault-tolerant mode.

- Other: It is highly recommended that you configure the load-balancer virtual server to return immediately to the calling client when the back-end services to which it forwards traffic are unavailable. This is preferred over the client disconnecting on its own after a timeout based on the TCP/IP settings on the client machine.

- SSL acceleration: This feature is required.

- Configuration of the virtual server or servers in the load balancer for the directory tier with a high value for the connection timeout for TCP connections: This value should be more than the maximum expected time over which no traffic is expected between Oracle Access Manager and the directory tier.

- Ability to preserve the client IP addresses: The load balancer must have the capability to insert the original client IP address of a request in an X-Forwarded-For HTTP header to preserve the client IP address.

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`.

3.3.2 Configuring a Load Balancer

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

1. Configure an HTTP monitor 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 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 WebCenter Content system, that is, specify a value greater than the longest period of time any of your requests to HTTP servers can take.

2. Configure a TCP/IP monitor for the WCCHOSTn nodes to detect failures in these nodes:

   - The monitor should be a TCP-Half-Open type.

   - The monitor should ping the nodes at the Oracle WebCenter Content Server port, 4444, every 5 seconds, with a timeout value of 16 seconds.

3. Create a pool of servers and assign the HTTP monitor created in Step 1 to the pool. This pool contains a list of servers and the ports that are included in the load-balancing definition. For example, for load balancing between the web hosts, you create a pool of servers that would direct requests to hosts WEBHOST1 and WEBHOST2 on port 7777.

4. Also create a pool of servers and assign the TCP/IP monitor created in step 2 to the pool, which would direct RIDC requests to hosts WCCHOST1 and WCCHOST2 on port 4444.

5. Create rules to determine whether or not a given host and service is available and assign it to the pool of servers described in Step 3.

6. Configure a virtual server in the load balancer for `admin.example.com:80`, and define the following rules for this virtual server:

   - Use your internal administration address as the virtual server address (`admin.example.com`). This address is typically not externalized.

   - Specify HTTP as the protocol.

   - Configure this virtual server with port 80. HTTP requests that go to port 80 should be redirected to port 7777 on the HTTP nodes.

   - Enable address and port translation.

   - Enable reset of connections when services, nodes, or both are down.

   - Optionally, create rules to allow access only to `/console` and `/em` on this virtual server.

   - Assign the pool created in step 3 to the virtual server.

7. Configure a virtual server in the load balancer for `wccinternal.example.com:80`, and define the following rules for this virtual server:

   - Use your internal Oracle WebCenter Content address as the virtual server address (`wccinternal.example.com`). This address is typically not externalized.

   - Specify HTTP as the protocol.

   - Configure this virtual server with port 80. HTTP requests that go to port 80 should be redirected to port 7777 on the HTTP nodes.

   - Enable address and port translation.

   - Enable reset of connections when services, nodes, or both are down.

   - Assign the pool created in step 3 to the virtual server.

   - Create rules to filter out access to `/console` and `/em` on this virtual server.

8. Configure a virtual server in the load balancer for `ucminternal.example.com:6300`, and define the following rules for this virtual server:

   - Use the internal address (`ucminternal.example.com`) as the virtual server address. This address is typically not externalized.

   - Specify TCP/IP as the protocol.

   - Configure this virtual server with port 6300. RIDC requests that go to port 6300 should be redirected to port 4444 on the Content Server nodes.

   - Enable address and port translation.

   - Enable reset of connections when services, nodes, or both are down.

   - Assign the pool created in step 3 to the virtual server, for RIDC requests.

After you configure the virtual hosts in Section 9.5, "Defining Virtual Hosts," you should be able to access the virtual host name addresses. If you cannot access them, review this procedure to ensure that it was completed correctly.

3.4 IP Addresses and Virtual IP Addresses

Configure the Administration Server and the Managed Servers to listen on different physical IP addresses and virtual IPs addresses, as illustrated in Figure 3–1. As this figure shows, each IP address and virtual IP address is attached to the Oracle WebLogic Server instance that uses it. VIP1 is failed manually to restart the Administration Server in WCCHOST2. If Oracle SOA Suite is configured to use with Imaging, WLS_SOA1 and WLS_SOA2 use VIP2 and VIP3 to fail over from WCCHOST1 to WCCHOST2 and from WCCHOST2 to WCCHOST1, 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 and from WCCHOST2 to WCCHOST1. Likewise, WLS_CPT1 and WLS_CPT2 use VIP6 and VIP7 for failovers.

For information about the WebLogic Server migration feature, see the *Oracle Fusion Middleware High Availability Guide*.

Physical IP addresses (nonvirtual) are fixed to each node. IP1 is a physical IP address of WCCHOST1 and is used as the listen address by the WLS_WCC1 server. IP2 is a physical IP address of WCCHOST2 and is used as the listen address by the WLS_WCC2 server.

The virtual IP address `db-scan.example.com` is the database Oracle Single Client Access Name (SCAN) address for a GridLink data source.

Figure 3–1   IP and Virtual IP Addresses Mapped to the Administration Server and Managed Servers
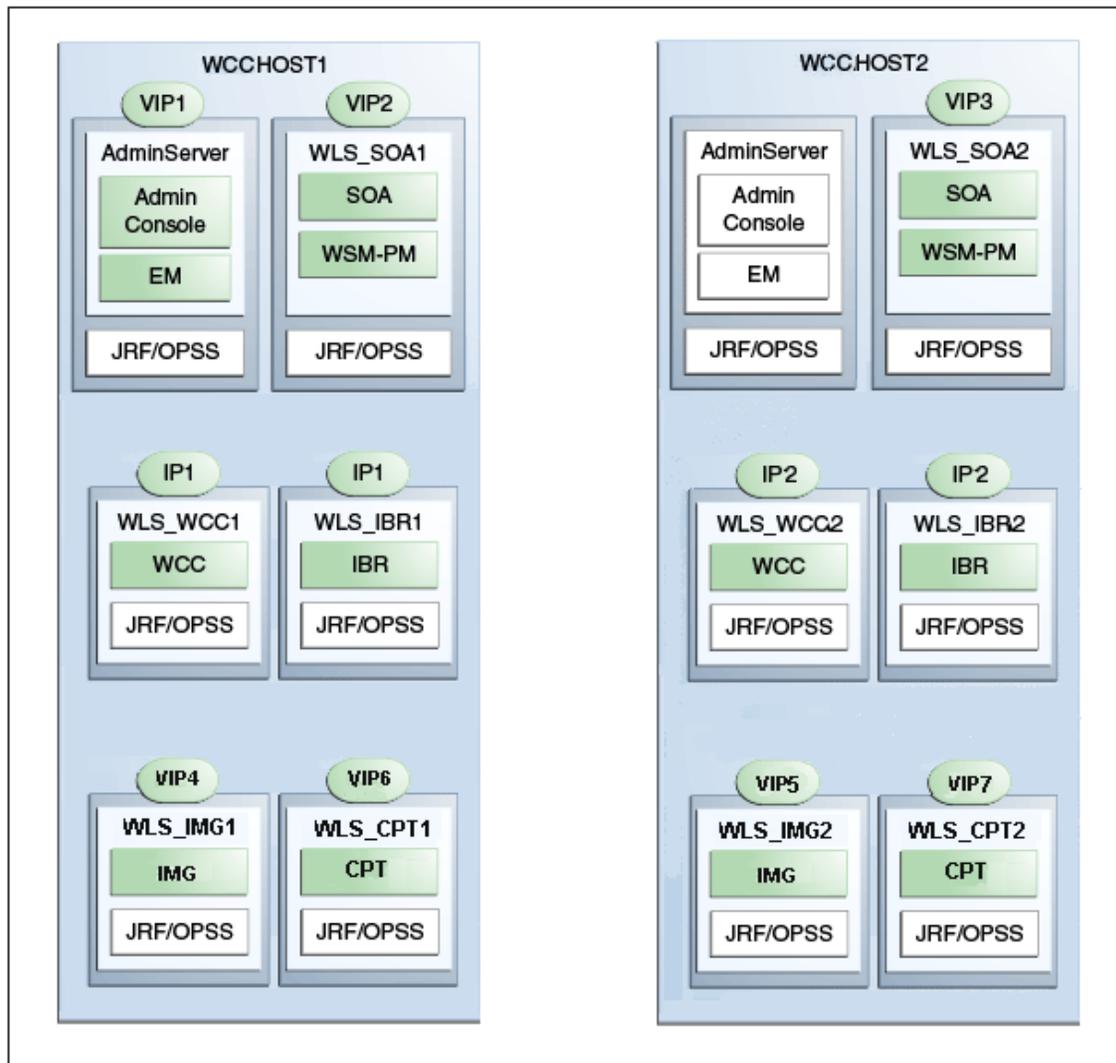
Table 3–1 provides descriptions of the various virtual hosts to which the virtual IP addresses are mapped.

Table 3–1   Virtual Hosts Mapped to Virtual IP Addresses

Virtual IP Address	Virtual Host Name	Description
VIP1	ADMINVHN	ADMINVHN is the virtual host name that is the listen address for the Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the Administration Server process is running (WCCHOST1 by default).
VIP2	WCCHOST1VHN1	WCCHOST1VHN1 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 the WLS_SOA1 process is running (WCCHOST1 by default).
VIP3	WCCHOST2VHN1	WCCHOST2VHN1 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 the WLS_SOA2 process is running (WCCHOST2 by default).

Table 3–1   (Cont.) Virtual Hosts Mapped to Virtual IP Addresses

Virtual IP Address	Virtual Host Name	Description
VIP4	WCCHOST1VHN2	WCCHOST1VHN2 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).
VIP5	WCCHOST2VHN2	WCCHOST2VHN2 is the virtual host name that maps to the listen address for WLS_IMG2 and fails over with server migration of this Managed Server. It is enabled on the node where WLS_IMG2 process is running (WCCHOST2 by default).
VIP6	WCCHOST1VHN3	WCCHOST1VHN3 is the virtual host name that maps to the listen address for WLS_CPT1 and fails over with server migration of this Managed Server. It is enabled on the node where WLS_CPT1 process is running (WCCHOST1 by default).
VIP7	WCCHOST2VHN3	WCCHOST2VHN3 is the virtual host name that maps to the listen address for WLS_CPT2 and fails over with server migration of this Managed Server. It is enabled on the node where WLS_CPT2 process is running (WCCHOST2 by default).
`db-scan.example.com`		`db-scan.example.com` is the database Oracle Single Client Access Name (SCAN) address for a GridLink data source.

3.5 Firewalls and Ports

Many Oracle Fusion Middleware components and services use ports. As an administrator, you must know the port numbers used by these services and 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 Oracle Web Tier and the application tier.

- FW2 refers to the firewall between the application tier and the data tier.

Table 3–2   Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Browser request	FW0	80	HTTP / Load Balancer	Inbound	Timeout depends on all HTML content and the type of process model used for Oracle SOA Suite.
Browser request	FW0	443	HTTPS / Load Balancer	Inbound	Timeout depends on all HTML content and the type of process model used for Oracle SOA Suite.
Browser request	FW1	80	HTTP / Load Balancer	Outbound (for intranet clients)	Timeout depends on all HTML content and the type of process model used for Oracle SOA Suite.

Table 3–2   (Cont.) Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Browser request	FW1	443	HTTPS / Load Balancer	Outbound (for intranet clients)	Timeout depends on all HTML content and the type of process model used for Oracle SOA Suite.
Callbacks and outbound invocations	FW1	80	HTTP / Load Balancer	Outbound	Timeout depends on all HTML content and the type of process model used for Oracle SOA Suite.
Callbacks and Outbound invocations	FW1	443	HTTPS / Load Balancer	Outbound	Timeout depends on all HTML content and the type of process model used for Oracle SOA Suite.
Oracle Notification Server (ONS)	FW2	6200	ONS	Both	Both required for Gridlink. An ONS server runs on each database server.
Load balancer to Oracle HTTP Server	n/a	7777	HTTP	n/a	See Section 3.3, "Load Balancers."
Load balancer to Remote Intradoc Client (RIDC)	FW1	6300	TCP/IP Unicast	n/a	The connection persists.
OHS registration with Administration Server	FW1	7001	HTTP/t3	Inbound	Set the timeout to a short period (5-10 seconds).
OHS management by Administration Server	FW1	OPMN port (6701) and OHS Admin Port (7779)	TCP and HTTP, respectively	Outbound	Set the timeout to a short period (5-10 seconds).
Oracle SOA Suite and Oracle WSM server access	FW1	8001 Range: 8000 - 8080	HTTP / WLS_SOAn	Inbound and Outbound	Timeout varies based on the type of process model used for Oracle SOA Suite.
Oracle WebCenter Content access	FW1	16200	HTTP / WLS_WCCn	Inbound	Browser-based access. Configurable session timeouts.
Oracle WebCenter Content: Imaging access	FW1	16000	HTTP / WLS_IMGn	Inbound	Browser-based access. Configurable session timeouts.
Oracle WebCenter Enterprise Capture access	FW1	16400	HTTP / WLS_CPTn	Inbound	Browser-based access. Configurable session timeouts.
Imaging connection to Oracle WebCenter Content	FW1	6300	TCP/IP Unicast	n/a	Persistent connection. Timeout configurable on Content Server.
Communication between SOA_Cluster members	n/a	8001	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.

Table 3–2   (Cont.) Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Communication between WCC_Cluster members	n/a	16200	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.
Communication between IMG_Cluster members	n/a	16000	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.
Communication between CPT_Cluster members	n/a	16400	TCP/IP Unicast	n/a	By default, this communication uses the same port as the server's listen address.
Session replication within a WebLogic Server cluster	n/a	n/a	n/a	n/a	By default, this communication uses the same port as the server's listen address.
Administration Console access	FW1	7001	HTTP / Administration Server and Oracle Enterprise Manager Fusion Middleware Control t3	Both	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).
Node Manager	n/a	5556	TCP/IP	n/a	n/a For actual values, see "Firewall and Port Configuration" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.
Access Server access	FW1	5575 (Oracle Access Manager 11*g*)	OAP	Inbound	For actual values, see "Firewall and Port Configuration" in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.
Database access	FW2	1521	SQL*Net	Both	Timeout depends on all database content and on the type of process model used for Oracle SOA Suite.
Coherence for deployment	n/a	8088 Range: 8000 - 8090		n/a	n/a
Oracle Internet Directory access	FW2	389	LDAP	Inbound	You should tune the directory server's parameters based on load balancer, and not the other way around.

Table 3–2   (Cont.) Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Oracle Internet Directory access	FW2	636	LDAP SSL	Inbound	You should tune the directory server's parameters based on load balancer, and not the other way around.
JOC for OWSM	n/a	9991 Range: 9988-9998	TCP/IP	n/a	n/a
Browser request	n/a	16250 16250	HTTP / WLS_IBRn	n/a	Browser-based access. Configurable session timeouts.

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

4

Preparing the File System for an Enterprise Deployment

This chapter describes how to prepare the 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 sections:

- 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, "Directory Structure and Configurations"
- Section 4.4, "Recommended Locations for Different Directories"
- Section 4.5, "Shared Storage Configuration"

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 this 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. Oracle WebCenter Content has two different domain setups, one for the Oracle WebCenter Content domain and one for the WebCenter Content user interface domains. The two domains have different file-system layouts.

Table 4–1 describes directory variables that represent directories in the application tier throughout this guide.

Table 4–1   Directory Variables for the Application Tier in the Oracle WebCenter Content Domain

Directory Variable	Description	Directory in the Reference Topology Application Tier

`ORACLE_BASE`	The directory path to the installation and configuration files for Oracle Fusion Middleware products.	`/u01/oracle`
		
		or
		
		`/u02/oracle`

`MW_HOME`	The directory path to a Middleware home, where Oracle Fusion Middleware products are installed. The Middleware home contains the WebLogic Server home (*WL_HOME*), the Oracle Common home (*ORACLE_COMMON_HOME*), and, optionally, the JDK home (`JAVA_HOME`) and one or more Oracle homes for Oracle Fusion Middleware components and products, including Oracle WebCenter Content (`WCC_ORACLE_HOME`). A Middleware home can reside on a local file system or on a remote shared disk that is accessible through Network File System (NFS).	`/u01/oracle/products/fmw_home`
`WL_HOME`	The directory path to a WebLogic Server home, which contains the installed files for Oracle WebLogic Server.	`/u01/oracle/products/fmw_home/wlserver_10.3`
`WCC_ORACLE_HOME`	The directory path to an Oracle home where Oracle WebCenter Content is installed.	`/u01/oracle/products/fmw_home/wcc_home`
`SOA_ORACLE_HOME`	The directory path to an Oracle home where Oracle SOA Suite is installed.	`/u01/oracle/products/fmw_home/soa`
`ORACLE_COMMON_HOME`	The directory path to the domain's Oracle Common home, which contains the binary and library files required for Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).	`/u01/oracle/products/fmw_home/oracle_common`
`JAVA_HOME`	This is the location where Oracle JRockit or another JDK is installed.	`/u01/oracle/products/fmw_home/JRockit_version`

Table 4–1   (Cont.) Directory Variables for the Application Tier in the Oracle WebCenter Content Domain

Directory Variable	Description	Directory in the Reference Topology Application Tier
ASERVER_HOME	The directory path to the primary location of the domain configuration for the WebLogic Server Administration Server, where the domain information and configuration artifacts are stored. Different Oracle WebLogic Servers can use different domain directories even when in the same node.	/u01/oracle/config/domains/WCCDomain
MSERVER_HOME	The directory path to the primary location of the domain configuration for the WebLogic Server Managed Servers, where the domain information and configuration artifacts are stored. Different Oracle WebLogic Servers can use different domain directories even when in the same node. This is a copy of the domain configuration used to start and stop Managed Servers.	/u02/oracle/config/domains/WCCDomain
APPLICATION_HOME	The directory path to the location of the application directory for the Administration Server and Managed Servers, local to each node.	/u01/oracle/config/applications/WCCDomain

Table 4–2 describes directory variables that represent directories in Oracle Web Tier throughout this guide.

Table 4–2   Directory Variables for Oracle Web Tier

Directory Variable	Description	Sample Value in Oracle Web Tier
WT_ORACLE_HOME	The directory path to the Oracle Web Tier Oracle home, which includes the binary and library files required for an Oracle Web Tier installation.	/u02/oracle/products/fmw_home/web_home
ORACLE_INSTANCE	The directory path to an Oracle instance directory, which contains updateable files, such as configuration files, log files, and temporary files. An Oracle instance contains one or more system components, such as Oracle Web Cache, Oracle HTTP Server, or Oracle Internet Directory.	/u02/oracle/config/web1 or /u02/oracle/config/web2
WEBGATE_ORACLE_HOME	The directory path to the WebGate installation.	/u02/oracle/products/fmw_home/WebGate_home

Table 4–3 describes directory variables that represent directories in the application tier of the WebCenter Content user interface domain throughout this guide.

Table 4–3   Directory Variables for the Application Tier in the WebCenter Content User Interface Domain

Directory Variable	Description	Sample Value in the Application Tier
WCCUI_MW_HOME	The directory path to a Middleware home, where Oracle Fusion Middleware products are installed. The Middleware home contains the WebLogic Server Home (*WCCUI_WL_HOME*), the Oracle Common home (WCCUI_*ORACLE_COMMON_HOME*), and, optionally, the JDK home (*WCCUI_JAVA_HOME*) and one or more Oracle homes for Oracle Fusion Middleware components and products, including WebCenter Content user interface. A Middleware home can reside on a local file system or on a remote shared disk that is accessible through Network File System (NFS).	/u01/oracle/products/fmw_home
WCCUI_WL_HOME	The directory path to a WebLogic Server home, which contains the installed files for Oracle WebLogic Server.	/u01/oracle/products/fmw_home/wlserver_10.3
WCCUI_ORACLE_COMMON_HOME	The directory path to the domain's Oracle Common home, which contains the binary and library files required for Oracle Enterprise Manager Fusion Middleware Control and Java Required Files (JRF).	/u01/oracle/products/fmw_home/oracle_common
WCCUI_JAVA_HOME	This is the location where Oracle JRockit or another JDK is installed. Value	/u01/oracle/products/fmw_home/JRockit_*version*
WCCUI_ASERVER_HOME	The directory path to the primary location of the domain configuration for the WebLogic Server Administration Server, where the domain information and configuration artifacts are stored. Different Oracle WebLogic Servers can use different domain directories even when in the same node.	/u01/oracle/config/domains/WCCUIDomain
WCCUI_MSERVER_HOME	The directory path to the primary location of the domain configuration for the WebLogic Server Managed Servers, where the domain information and configuration artifacts are stored. Different Oracle WebLogic Servers can use different domain directories even when in the same node. This is a copy of the domain configuration used to start and stop Managed Servers.	/u02/oracle/config/domains/WCCUIDomain
WCCUI_APPLICATION_HOME	The directory path to the location of the application directory for the Administration Server and Managed Servers, local to each node.	/u01/oracle/config/applications/WCCUIDomain

> **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 $MW_HOME to refer to /u01/oracle/products/fmw_home (that is, the recommended Middleware home location, represented by *MW_HOME* in directory paths).

4.3 Directory Structure and Configurations

The following diagrams and tables illustrate the recommended directory structure and shared storage.

Figure 4–1 shows the directory structure for the Administration Server domain directories.

Figure 4–1   File Layout for Product Binaries and ASERVER Domain Directories (Shared Storage)
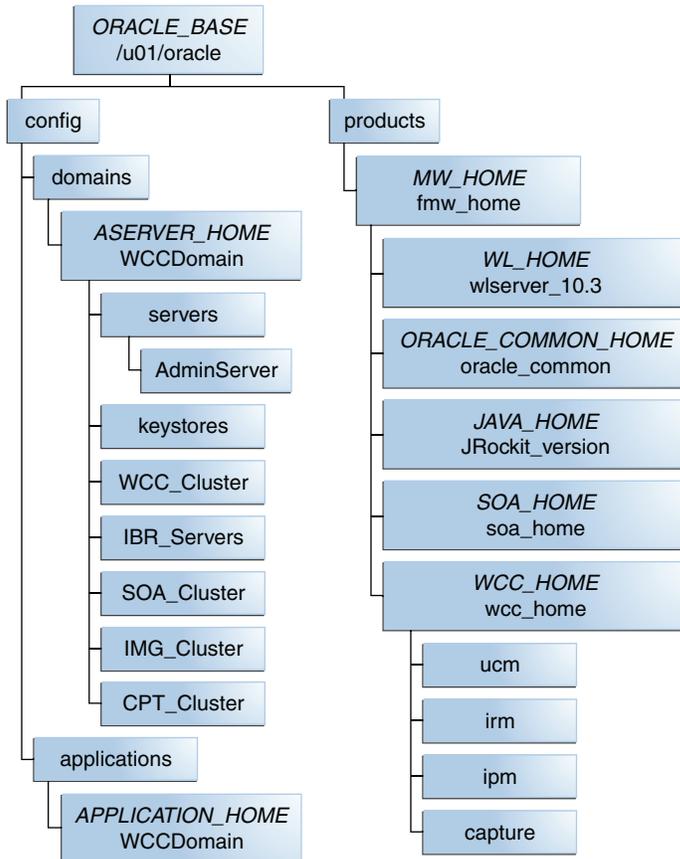
Figure 4–2 shows the directory structure for the Managed Server domain directories.

Figure 4–2   File Layout for MSERVER Domain Directories
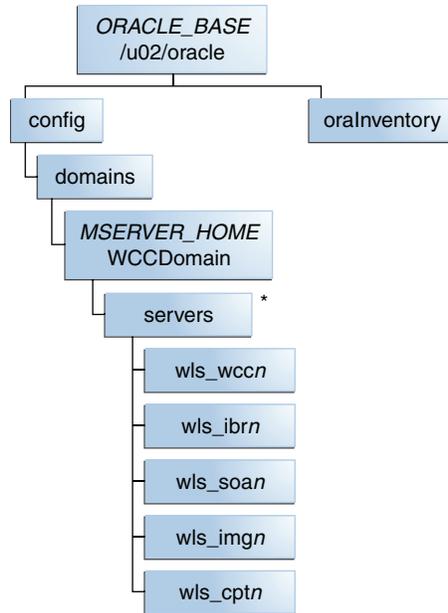
* All WebLogic Server Managed Servers are created during domain extension, after unpacking to the local disk *MSERVER_HOME.*

Figure 4–3 shows the directory structure for the web tier.

Figure 4–3   File Layout for Web Tier Instance Directories in Local Storage
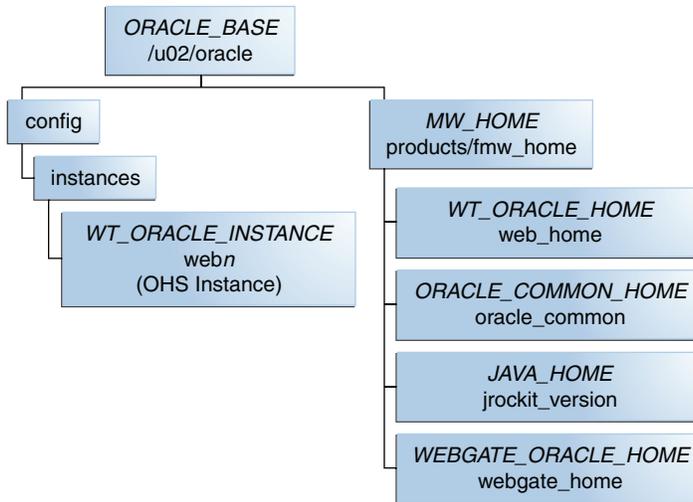
Figure 4–4 shows the directory structure for the WebCenter Content user interface Administration Server domain directories.

Figure 4–4   File Layout for Product Binaries and ASERVER Domain Directories for WebCenter Content User Interface (Shared Storage)
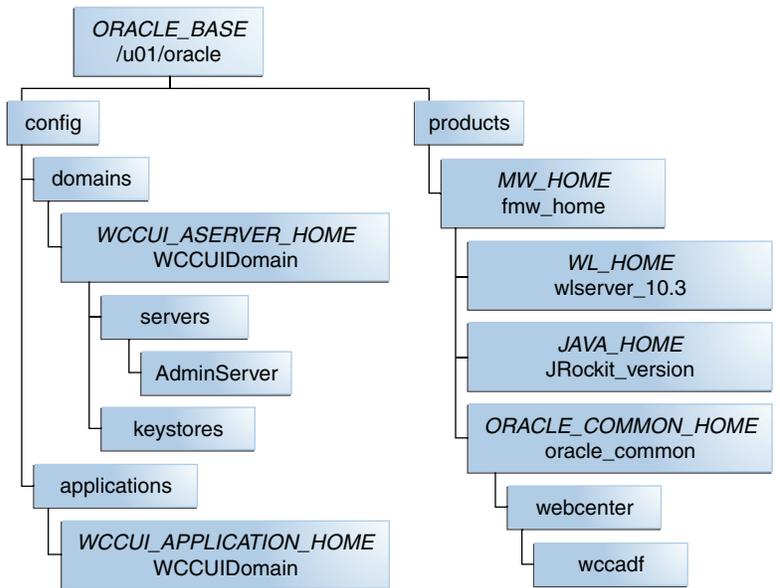
* Oracle ADF patched to 11.1.2.4 version

Figure 4–5 shows the directory structure for the WebCenter Content user interface Managed Server domain directories.

Figure 4–5   File Layout for MSERVER Domain Directories for the WebCenter Content User Interface
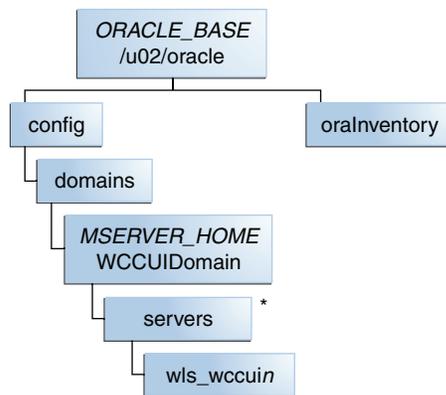
* All WebLogic Server Managed Servers are created during domain extension, after unpacking to the local disk *MSERVER_HOME.*

Table 4–4 summarizes the directory structure for an Oracle WebLogic Server domain that includes Oracle WebCenter Content and Oracle SOA Suite Managed Servers that share storage.

Table 4–4   Contents of Shared Storage for the Oracle WebCenter Content Domain

WebLogic Servers	Type of Data	Volume in Shared Storage	Mount Point	Files and Subdirectories	Mount Host
Administration Server and all Managed Servers running on WCCHOST1	FMW Products Installation	VOL1a	/u01/oracle/products	This volume is mounted as local storage for WCCHOST1. VOL1a contains all installed binary files and subdirectories used by any WebLogic server running on WCCHOST1.	WCCHOST1
Administration Server and all Managed Servers running on WCCHOST2	FMW Products Installation	VOL1b	/u01/oracle/products	This volume is mounted as local storage for WCCHOST2. VOL1b contains all installed binary files and subdirectories used by any WebLogic server running on WCCHOST2.	WCCHOST2
Administration Server	Domain configuration	VOL1c	/u01/oracle/config	This shared volume is used for the Administration Server domain configuration and cluster-related subdirectories. (WCCHOST1 and WCCHOST2 mount VOL1c.)	WCCHOST1 WCCHOST2
WLS_WCC1, WLS_IBR1, WLS_SOA1, WLS_IMG1, WLS_CPT1	Domain configuration	VOL1d	/u02/oracle	This volume is mounted on local storage for OraInventory and Managed Server domain configuration. WCCHOST1 mounts VOL1d.	WCCHOST1

Table 4–4   (Cont.) Contents of Shared Storage for the Oracle WebCenter Content Domain

WebLogic Servers	Type of Data	Volume in Shared Storage	Mount Point	Files and Subdirectories	Mount Host
WLS_WCC2, WLS_IBR2, WLS_SOA2, WLS_IMG2, WLS_CPT2	Domain configuration	VOL1e	/u02/oracle	This volume is mounted on local storage for OraInventory and Managed Server domain configuration. WCCHOST2 mounts `VOL1e`.	WCCHOST2
Oracle Web Tier	Web tier installation and configuration	VOL1f	/u02/oracle	This volume is mounted on local storage for OHS installation. WCCHOST1 mounts `VOL1f`.	WEBHOST1
Oracle Web Tier	Web tier installation and configuration	VOL1g	/u02/oracle	This volume is mounted on local storage for OHS installation. WCCHOST2 mounts `VOL1g`.	WEBHOST2

Table 4–5 summarizes the directory structure for an Oracle WebLogic Server domain that includes the WebCenter Content user interface.

Table 4–5   Contents of Shared Storage for the WebCenter Content User Interface Domain

WebLogic Servers	Type of Data	Volume in Shared Storage	Mount Point	Files and Subdirectories	Mount Host
Administration Server and all Managed Servers running on WCCUIHOST1	FMW Products Installation	VOL2a	u01/oracle/products	This volume is mounted as local storage for WCCUIHOST1. VOL2a contains all installed binary files and subdirectories used by any WebLogic server running on WCCUIHOST1. (WCCUIHOST1 mounts VOL2a.)	WCCUIHOST1
Administration Server and all Managed Servers running on WCCUIHOST2	FMW Products Installation	VOL2b	u01/oracle/products	This volume is mounted as local storage for WCCUIHOST2. VOL2b contains all installed binary files and subdirectories used by any WebLogic server running on WCCUIHOST2. (WCCUIHOST2 mounts VOL2b.)	WCCUIHOST2
Administration Server	Domain configuration	VOL2c	u01/oracle/config	This shared volume is used for the Administration Server domain configuration. (WCCUIHOST1 and WCCUIHOST2 mount VOL2c.)	WCCUIHOST1 WCCUIHOST2
WLS_WCCUI1	Domain configuration	VOL2d	/u02/oracle	This volume is mounted on local storage for OraInventory and Managed Server domain configuration. (WCCUIHOST1 mounts VOL2d.)	WCCUIHOST1
WLS_WCCUI2	Domain configuration	VOL2e	/u02/oracle	This volume is mounted on local storage for OraInventory and Managed Server domain configuration. (WCCHOST2 mounts VOL2e.)	WCCUIHOST2

4.4 Recommended Locations for Different Directories

The following sections describe some basic recommendations for using shared storage in an enterprise deployment topology:

- Section 4.4.1, "Shared Storage Recommendations for Binary (Oracle Home) Directories"

- Section 4.4.2, "Shared Storage Recommendations for Domain Configuration Files"

- Section 4.4.3, "Directory Locations in the Reference Topology"

4.4.1 Shared Storage Recommendations for Binary (Oracle Home) Directories

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

- Section 4.4.1.1, "About the Binary (Oracle Home) Directories"

- Section 4.4.1.2, "About Sharing a Single Oracle Home for Multiple Domains"

- Section 4.4.1.3, "About Using Redundant Binary (Oracle Home) Directories"

4.4.1.1 About the Binary (Oracle Home) Directories

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

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

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

For more information about the structure and contents of an Oracle Fusion Middleware Oracle home, see *Concepts*.

4.4.1.2 About Sharing a Single Oracle Home for Multiple Domains

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

> **Note:** The domain directories of the Managed Servers can reside in local or shared storage. If the WebCenter Content Managed Servers or Inbound Refinery Managed Servers use shared storage, they should use different volumes because each Managed Server uses a node-specific file.

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

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

`MW_HOME/oui/bin/attachHome.sh`

In the Oracle WebCenter Content reference topology for an enterprise deployment, *MW_ HOME* is the `/u01/oracle/products/fmw_home` directory.

For more information about the Oracle Inventory, see "Oracle Universal Installer Inventory" in the *Oracle Universal Installer and OPatch User's Guide*.

4.4.1.3 About Using Redundant Binary (Oracle Home) Directories

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

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

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

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

4.4.2 Shared Storage Recommendations for Domain Configuration Files

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

- Section 4.4.2.1, "About Oracle WebLogic Server Administration and Managed Server Domain Configuration Files"

- Section 4.4.2.2, "Shared Storage Requirements for Administration and Managed Server Domain Configuration Files"

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

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

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

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

4.4.2.2 Shared Storage Requirements for Administration and Managed Server Domain Configuration Files

Oracle recommends creating two copies of the domain configuration files:

- One copy is for the Administration Server configuration files.

  You install this directory on shared storage and mount it exclusively to the host that is running the Administration Server.

  In the event of the failure of that host, you can mount the directory on a different host, and have the Administration Server started on that host.

- The other copy is for the Managed Server configuration files.

  The domain directories of the Managed Servers can reside in local or shared storage. If the WebCenter Content Managed Servers or the Inbound Refinery Managed Servers use shared storage, they should use different volumes because they use node-specific files, such as the following ones:

  - WebCenter Content uses `MSERVER_HOME`/ucm/cs/bin/intradoc.cfg.

    In the reference topology, `MSERVER_HOME` is the `/u02/oracle/config/domains/WCCDomain` directory.

  - Inbound Refinery uses `MSERVER_HOME`/ucm/ibr/bin/intradoc.cfg.

  Sharing domain directories for Managed Servers facilitates the scale-out procedures. However, sharing the Managed Server configuration files could have a performance impact.

  As a result, the deployment you decide upon should conform to the requirements (if any) of the storage system. Some storage systems offer configuration options to facilitate multiple machines mounting the same shared volume.

  The configuration steps provided for this reference topology are based on the assumption that a local domain directory for each node is used for each Managed Server.

4.4.3 Directory Locations in the Reference Topology

Based on the previous assumptions, 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."

Shared storage is the path on the share (volume) on the storage device. The shared storage locations are examples and can be changed as long as the provided mount points are used. Oracle recommends this structure on the shared storage device for consistency and simplicity.

4.4.3.1 Directory Locations for the Oracle WebCenter Content Domain

The following file-system locations are recommended for directories in the Oracle WebCenter Content domain:

- Middleware home (*MW_HOME*)

  `/u01/oracle/products/fmw_home`

> **Note:** When just one volume is available in shared storage, you can provide redundancy by using different directories to protect from accidental file deletions and for patching purposes. You could make two Middleware homes available, for example, at these directories: `/u01/oracle/products/fmw_home1` and `/u01/oracle/products/fmw_home2`. These Middleware homes would be mounted on the same mount point in all nodes.

- WebLogic Server home (*WL_HOME*)

  `/u01/oracle/products/fmw_home/wlserver_10.3`

- Oracle WebCenter Content Oracle home (*WCC_ORACLE_HOME*)

  `/u01/oracle/products/fmw_home/wcc_home`

- Oracle Common home (*ORACLE_COMMON_HOME*)

  `/u01/oracle/products/fmw_home/oracle_common`

- Domain directory for the Administration Server (*ASERVER_HOME*)

  `/u01/oracle/config/domains/WCCDomain`

  The Fusion Middleware Configuration Wizard adds the `WCCDomain` directory.

- Domain directory for the Managed Servers (*MSERVER_HOME*)

  `/u02/oracle/config/domains/WCCDomain`

  The Fusion Middleware Configuration Wizard adds the `WCCDomain` directory.

- Location of all component cluster-related files, including JMS file-based stores and tlogs

  All component cluster-related files and Inbound Refinery files go under one shared storage volume mounted to both hosts. A subdirectory for each cluster and a subdirectory for the Inbound Refinery servers are created under *ASERVER_HOME*, as follows:

  ```
  /u01/oracle/config/domains/WCCDomain/WCC_Cluster
  /u01/oracle/config/domains/WCCDomain/SOA_Cluster
  /u01/oracle/config/domains/WCCDomain/IMG_Cluster
  /u01/oracle/config/domains/WCCDomain/CPT_Cluster
  /u01/oracle/config/domains/WCCDomain/IBR_Servers
  ```

  In the reference topology, *ASERVER_HOME* is the `/u01/oracle/config/domains/WCCDomain` directory.

- Location of the application directory for the Administration Server and Managed Servers

  `/u01/oracle/config/applications/WCCDomain`

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

- Web Tier Oracle home (*WT_ORACLE_HOME*)

  `/u02/oracle/products/fmw_home/web_home`

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

- Oracle HTTP Server Oracle instance (*OHS_ORACLE_INSTANCE*)

  `/u02/oracle/products/fmw_home/ohs_instance_name`

4.4.3.2 Directory Locations for the WebCenter Content User Interface Domain

The following file-system locations are recommended for directories in the WebCenter Content user interface domain:

- Middleware home for the WebCenter Content user interface (*WCCUI_MW_HOME*)

  `/u01/oracle/products/WCCUI_MW_HOME`

- WebLogic Server home for the WebCenter Content user interface (*WCCUI_WL_HOME*)

  `/u01/oracle/products/WCCUI_MW_HOME/wlserver_10.3`

- Oracle home for the WebCenter Content user interface (*WCCUI_ORACLE_HOME*)

  `/u01/oracle/products/WCCUI_MW_HOME/wccui_home`

- Oracle Common home for the WebCenter Content user interface (*WCCUI_ORACLE_COMMON_HOME*)

  `/u01/oracle/products/WCCUI_MW_HOME/oracle_common`

- WebCenter Content user interface domain directory for the Administration Server (*WCCUI_ASERVER_HOME*)

  `/u01/oracle/config/domains/WCCUIDomain`

  The Fusion Middleware Configuration Wizard adds the `WCCUIDomain` directory.

- Domain directory for the Managed Servers (*WCCUI_MSERVER_HOME*)

  `/u02/oracle/config/domains/WCCUIDomain`

  The Fusion Middleware Configuration Wizard adds the `WCCUIDomain` directory.

- Location of all component cluster-related files, including JMS file-based stores and tlogs

  All component cluster-related files go under one shared storage volume mounted to both hosts. A subdirectory for the WebCenter Content user interface cluster is created under *WCCUI_ASERVER_HOME*, as follows:

  `/u01/oracle/config/domains/WCCUIDomain/WCCUI_Cluster`

- Location of application directory for the Administration Server and Managed Servers in the WebCenter Content user interface domain

  `/u01/oracle/config/applications/WCCUIDomain`

4.5 Shared Storage Configuration

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.

> **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*.

In the commands, `nasfiler` is the shared storage filer.

From WCCHOST1:

```
mount nasfiler:/export/wcc_edg/vol1a /u01/oracle/products/fmw_home -t nfs
```

From WCCHOST2:

```
mount nasfiler:/export/wcc_edg/vol2a /u01/oracle/products/fmw_home -t nfs
```

Validation of 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
```

5

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 sections:

- 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, "Creating Database Schemas"

- 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 Oracle Identity Management database, which is used in the Oracle 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 1–2. 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

For the Oracle WebCenter Content reference topology, Oracle Database 11*g* is recommended. Table 5–1 provides a summary of the database schemas. Which database or databases you use depends on the topology that you are implementing.

Table 5–1   Mapping Between Databases and Schemas

Database Name	Database Hosts	Service Name	Schemas in Database
wccdb.example.com	WCCDBHOST1 WCCDBHOST2	wccedg.example.com	WCC_MDS WCC_IAU WCC_OPSS WCC_OCS WCC_IPM WCC_CAPTURE WCC_SOAINFRA WCC_ORASDPM

The Oracle Metadata Services (MDS) Repository is a particular type of repository that contains metadata for some Oracle Fusion Middleware components. It can also include custom Java EE applications developed by your organization.

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 WCCDBHOST1 and WCCDBHOST2 in the data tier, note the following requirements:

- **Oracle Clusterware**

  For 11*g* Release 1 (11.1) for Linux, see the *Oracle Grid Infrastructure Installation Guide*.

- **Oracle Real Application Clusters**

  For 11*g* Release 1 (11.1) for Linux, see the *Oracle Real Application Clusters Installation Guide for Linux and UNIX*.

- **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 11*g* Release 1 (11.1.1.*x*)" product area on the Oracle Fusion Middleware Supported System Configurations page:

http://www.oracle.com/technetwork/middleware/ias/downloads/fusion-certification-10 0350.html

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

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

Notes:

- Oracle WebCenter Content requires that the database used to store its metadata (11*g*) supports the AL32UTF8 character set. Check the database documentation for information on choosing a character set for the database.

- 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 11*g*R2 (11.2 or later, Enterprise Edition).

- Oracle Database 11*g* is required for using Oracle Enterprise Capture because Capture uses Oracle Platform Security Services (OPSS), which works only with Oracle Database for its schema.

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 5–2   Required Initialization Parameters

Configuration	Parameter	Required Value	Parameter Class
Oracle SOA Suite	PROCESSES	400 or greater	Static
Oracle WebCenter Content	PROCESSES	100 or greater	Static
Oracle SOA Suite and Oracle WebCenter Content	PROCESSES	500 or greater	Static

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

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

```
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. For details on parameter files, server parameter files, and how to change a parameter value, see the *Oracle Database Administrator's Guide*.

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 an Oracle Database 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*.

Runtime 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 11*g* Release 1 (11.1), use the DBMS_SERVICE package for this modification. For Oracle Database 11*g* Release 2 (11.2), use the Server Control Utility (SRVCTL) instead.

The Oracle WebCenter Content installation is configured to use the service wccedg.example.com.

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

This section includes the following topics:

- Section 5.3.1, "Creating Database Services for 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 11g Release 1 (11.1) Databases

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

To create and modify an 11.1 database service:

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

   ```
   sqlplus "sys/password as sysdba"

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

   > **Notes:**
   >
   > - For the service name of an Oracle RAC database, use lowercase letters, followed by the domain name. For example:
   >
   >   wccedg.example.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:

```
srvctl start service -d wccdb -s wccedg.example.com
```

3. Start the service:

```
srvctl start service -d wccdb -s wccedg.example.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>EXECUTE DBMS_SERVICE.MODIFY_SERVICE (service_name =>
'wccedg.example.com',goal => DBMS_SERVICE.GOAL_THROUGHPUT, clb_goal =>DBMS_
SERVICE.CLB_GOAL_SHORT);

SQL>EXECUTE DBMS_SERVICE.MODIFY_SERVICE (service_name => 'wccedg.example.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 11*g* Release 2 (11.2) database services using the `srvctl` command.

To create and modify an 11.2 database service:

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

```
srvctl add service -d wccdb -s wccedg.example.com -r wccdb1,wccdb2 -q FALSE -m
NONE -e SELECT -w 0 -z 0
```

Descriptions of the command-line arguments follow.

Option	Argument
-d	Unique name of the database
-s	Service name
-r	List of preferred instances, separated by commas
-q	AQ HA notifications (`TRUE` or `FALSE`)
-e	Failover type (`NONE`, `SESSION`, or `SELECT`)
-m	Failover method (`NONE` or `BASIC`)
-w	Failover delay (integer)
-z	Failover retries (integer)

2. Start the service with the `srvctl start service` command:

```
srvctl start service -d wccdb -s wccedg.example.com
```

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

```
srvctl modify service –d wccdb –s wccedg.example.com –B SERVICE_TIME –j SHORT

srvctl modify service –d wccdb –s wccedg.example.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*.

4. Validate that the service started, with the `srvctl status service` command:

```
srvctl status service –d wccdb –s wccedg.example.com
Service wccedg.example.com is running on instance(s) wccdb1,wccdb2
```

5. Validate that the service was created correctly, with the `srvctl config service` command:

```
srvctl config service –d wccdb –s wccedg.example.com
Service name: wccedg.example.com
Service is enabled
Server pool: wccdb_wccedg.example.com
Cardinality: 2
Disconnect: false
Service role: PRIMARY
Management policy: AUTOMATIC
DTP transaction: false
AQ HA notifications: false
Failover type: SELECT
Failover method: NONE
TAF failover retries: 0
TAF failover delay: 0
Connection Load Balancing Goal: LONG
Runtime Load Balancing Goal: NONE
TAF policy specification: NONE
Edition:
Preferred instances: wccdb1,wccdb2
Available instances:
```

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

5.4 Creating Database Schemas

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 11*g* Release 1 (11.1.1.9) in this enterprise deployment, you must use RCU 11*g* Release 1 (11.1.1.9).

To load the Oracle Fusion Middleware Repository into a database:

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. On the Welcome screen (if displayed), click **Next**.

3. On the Create Repository screen, select **Create** to load component schemas into a database. Click **Next**.

4. On the Database Connection Details screen (Figure 5–1), enter the connect information for your database:

   - **Database Type**: Choose **Oracle Database**.

   - **Host Name**: Specify the name of the node on which the database resides. For the Oracle RAC database, specify the VIP name, scan address, or one of the node names as the host name; for example, `dbscan.example.com`.

   - **Port**: Specify the listen port number for the database: 1521.

   - **Service Name**: Specify the service name of the database (`wccedg.example.com`).

   - **Username**: Specify the name of the user with `DBA` or `SYSDBA` privileges: `SYS`.

   - **Password**: Enter the password for the `SYS` user.

   - **Role**: Choose the database user's role from the list: **SYSDBA** (required by the `SYS` user).

   Click **Next**.

Figure 5–1   Database Connection Details Screen
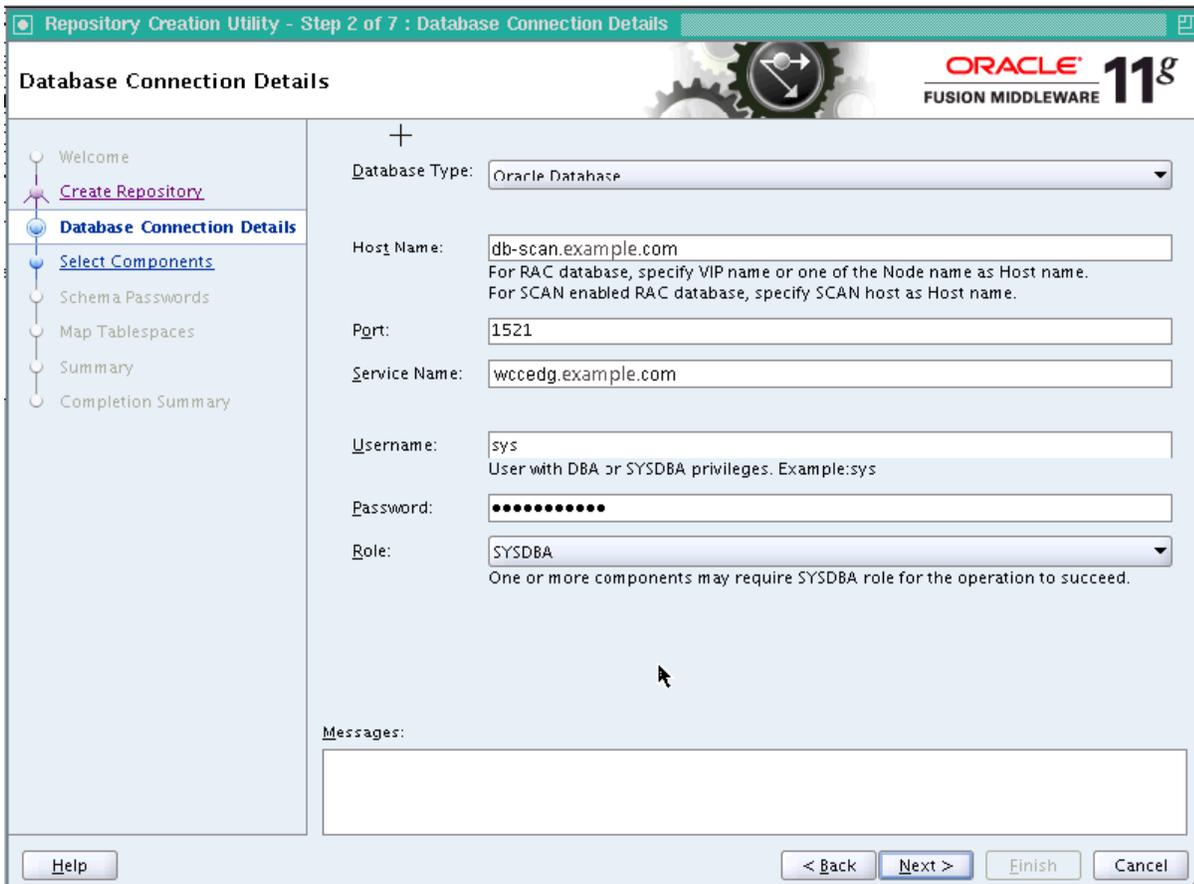
5. If your database is not using the UTF-8 character set, you will see a warning message indicating that there may be data loss if you are going to use the database for multilingual support. If you are not planning to use multilingual support, then you can click **Ignore**. Otherwise, click **Stop**.

6. On the Select Components screen (Figure 5–2), perform the following steps:

   ■ Select **Create a new Prefix**, and enter a prefix to use for the database schemas; for example WCC. 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 appropriate components from the following table for the topology you are using.

Figure 5–2   Select Components Screen
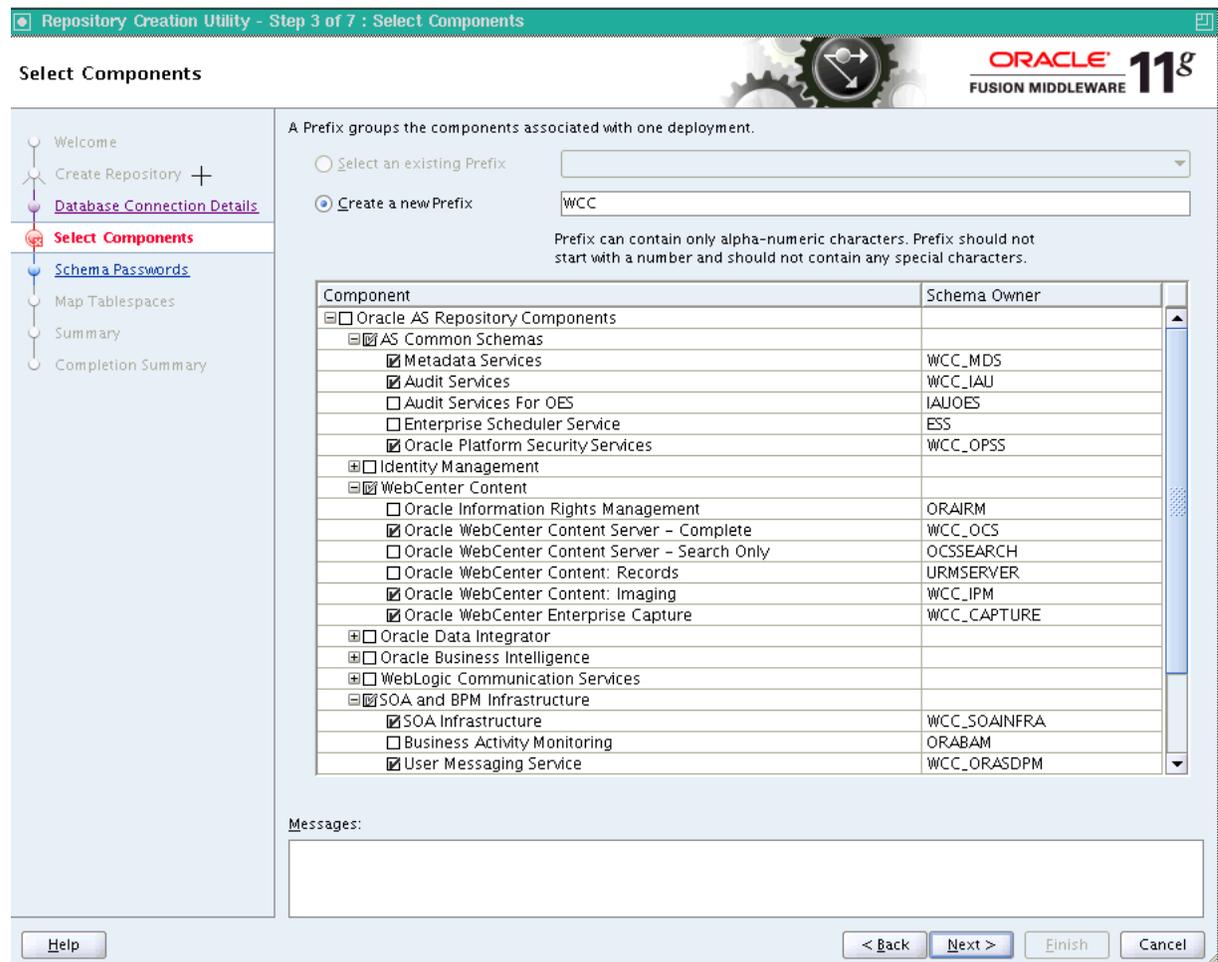
Table 5–3 shows which RCU components to select for the Oracle WebCenter Content feature sets you are using.

Table 5–3   RCU Components for an Oracle WebCenter Content Topology

Component Group	RCU Components to Select	Schema Names
AS Common Services	Metadata Services	WCC_MDS
	Audit Services	WCC_IAU
	Oracle Platform Security Services	WCC_OPSS
WebCenter Content	Oracle WebCenter Content Server - Complete	WCC_OCS
	Oracle WebCenter Content: Imaging	WCC_IPM
	Oracle WebCenter Enterprise Capture	WCC_CAPTURE
SOA and BPM Infrastructure	SOA Infrastructure	WCC_SOAINFRA
	User Messaging Service	WCC_ORASDPM

The MDS schema is necessary for the WebCenter Content user interface. This schema can be in the same database as the other schemas for the enterprise deployment reference topology. However, if WS_Policy is used in an Oracle WebCenter Content setup, which would require an MDS schema to implement the WS_Policy, then the WebCenter Content user interface requires its own MDS schema. You can create a new schema for MDS in the same database, using a different prefix.

Oracle Platform Security Services (OPSS) works only with Oracle Database 11*g* for its schema. The OPSS schema is necessary for a cluster setup (unless you are using Oracle Internet Directory and are going to reassociate the security store using it).

Either an OPSS schema or Oracle Internet Directory is necessary for a Capture cluster because the `system-jazn-data.xml` file is not sufficient for a cluster setup. If the security store is not in either the OPSS schema in the database or Oracle Internet Directory, the nodes in a two-node cluster get out of sync because the `system-jazn-data.xml` file on the second node in the cluster gets overwritten. Node Manager will sync the data from the first node and overwrite the file on the second node. With the OPSS schema or Oracle Internet Directory, the application data is preserved in a shared location to which both nodes have access.

If you use OPSS, a data source for it must be created manually after the domain is created.

Click **Next**.

7. On the Schema Passwords screen (Figure 5–3), select **Specify different passwords for all schemas**, and click **Next**. On the subsequent screen refresh, enter a schema passwords for each component.

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

Figure 5–3   Schema Passwords Screen

8. On 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. On the Summary screen, click **Create**.

10. On 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:

    ORACLE_HOME/bin/sqlplus

    Log in as the WCC_OCS user, and enter the password. You can perform a simple verification by querying the schema version registry:

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

    VERSION STATUS
    ---------------------------------------
    11.1.1.9.0 VALID
    ```

> **Note:** Oracle recommends using the database used for Oracle Identity Management (see Chapter 18, "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 preceding steps using the Oracle Identity Management database information, but select only **AS Common Schemas: Metadata Services** on the Select Components screen (step 6).

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. Oracle recommends that you use Oracle Recovery Manager for the database, particularly if the database was created using Oracle ASM. If possible, you can also perform a cold backup using operating system tools such as `tar`.

6

Preparing the Servers for an Enterprise Deployment

This chapter describes how to prepare the servers for an enterprise deployment.

This chapter includes the following sections:

- Section 6.1, "Overview of Preparing the Servers"
- Section 6.2, "Verifying Your Server and Operating System"
- Section 6.3, "Meeting the Minimum Hardware Requirements"
- Section 6.4, "Meeting Operating System Requirements"
- Section 6.5, "Enabling Unicode Support"
- Section 6.6, "Enabling Virtual IP Addresses"
- Section 6.7, "Configuring Users and Groups"

6.1 Overview of Preparing the Servers

Before you deploy Oracle Fusion Middleware on new hardware, you should set up the servers you plan to use so that the Oracle Software can work with optimum performance. Specifically, you should verify the following configuration:

- The servers are running on a certified operating system with the required software patches installed.
- You have configured the UNIX Kernel correctly.
- You have created users and groups to own the Oracle software.

The settings in this chapter are only a guide. After using your Oracle software, you should use operating system utilities to tune the configuration to ensure that you are maximizing the potential of your servers.

Table 6.1 lists the hosts on which the servers run in the Oracle WebCenter Content enterprise deployment topology.

Table 6–1   Host Machines

Host Name
WCCHOST1
WCCHOST2
WEBHOST1
WEBHOST2
WCCUIHOST1
WCCUIHOST2

6.2 Verifying Your Server and Operating System

Ensure that the server and operating system that you plan to use is are a certified combination for the products you plan to use. For details, see the Oracle Certification Matrix.

6.3 Meeting the Minimum Hardware Requirements

To use a server in an Oracle enterprise deployment, you must verify that it meets the minimum specification described in Section 1.2, "Hardware Requirements for an Enterprise Deployment on a Linux System." If you plan to use a different deployment architecture, such as one with more or fewer components deployed on a different number of machines, check the *Oracle Fusion Middleware System Requirements and Specifications* to ensure that you have the minimum specification to support the products you plan to deploy on these servers.

If you are deploying to a virtual server environment, such as Oracle Exalogic, ensure that each of the virtual servers meets the minimum requirements.

Ensure that you have sufficient local disk space and that shared storage is configured as described in Chapter 4, "Preparing the File System for an Enterprise Deployment."

Allow sufficient swap space and temporary space:

- Swap Space: 500 MB minimum

- Temporary Space: 500 MB minimum in `/tmp`.

6.4 Meeting Operating System Requirements

Before starting your operating system provisioning, perform the following tasks:

1. Install a certified operating system.

2. Install all necessary patches and packages.

The following topics describe configuration tasks for meeting the Oracle software requirements for a UNIX or Linux operating system:

- Configuring Kernel Parameters

- Setting the Open File Limit

- Setting Shell Limits

- Configuring Local Hosts File

6.4.1 Configuring Kernel Parameters on a UNIX or Linux System

Oracle recommends that you tune the following kernel parameter and shell-limit values to optimize the performance of a production database system. For more information about tuning kernel parameters, see your operating system documentation.

Kernel parameters must be set to at least the minimum values in the following table for all nodes in a cluster.

The values in the following table are the current Linux recommendations. For more information, see the *Oracle Fusion Middleware System Requirements and Specifications*. If you are deploying a database onto the host, you might need to modify additional kernel parameters.

Table 6–2   UNIX Kernel Parameters

Parameter	Value
kernel.sem	256 32000 100 142
kernel.shmmax	4294967295

To set these kernel parameters:

1. Log in as `root`, and add or amend the entries in the file `/etc/sysctl.conf`.

2. Save the file.

3. Activate the changes by issuing this command:

```
/sbin/sysctl -p
```

6.4.2 Setting the Open File Limit on a UNIX or Linux System

On all UNIX operating systems, the minimum Open File Limit should be 4096.

> **Note:** The following examples are for Linux operating systems. Consult your operating system documentation to determine the commands to be used on your system.

You can see how many files are open with the following command:

```
/usr/sbin/lsof | wc -l
```

To check your open file limits, use the commands below.

C shell:

```
limit descriptors
```

Bash:

```
ulimit -n
```

6.4.3 Setting Shell Limits on a UNIX or Linux System

To change the shell limits, log in as `root` and edit the `/etc/security/limits.conf` file, and add the following lines:

```
* soft  nofile  4096
* hard  nofile  65536
* soft  nproc   2047
* hard  nproc   16384
```

After editing the file, reboot the machine.

For the latest suggested values, see the *Oracle Fusion Middleware System Requirements and Specifications*.

6.4.4 Configuring Local Hosts File on a UNIX or Linux System

Before you begin the installation of the Oracle software, ensure that your local `hosts` file is formatted like this:

```
IP_Address Fully_Qualified_Name Short_Name
```

6.5 Enabling Unicode Support

Your operating system configuration can influence the behavior of characters supported by Oracle Fusion Middleware products.

On UNIX operating systems, Oracle highly recommends that you enable Unicode support by setting the `LANG` and `LC_ALL` environment variables to a locale with the UTF-8 character set. This enables the operating system to process any character in Unicode. Oracle SOA Suite technologies, for example, are based on Unicode.

If the operating system is configured to use a non-UTF-8 encoding, Oracle SOA Suite components may function in an unexpected way. For example, a non-ASCII file name might make the file inaccessible and cause an error. Oracle does not support problems caused by operating system constraints.

6.6 Enabling Virtual IP Addresses

The enterprise deployment requires that certain hosts, such as those running the WebLogic Server Administration Server or Oracle SOA Suite Managed Servers, use virtual IP addresses. You must enable the appropriate IP address on each server.

Section 3.4, "IP Addresses and Virtual IP Addresses," describes the mapping of IP addresses to servers.

6.6.1 Determining Virtual IP Addresses to Enable

Virtual IP addresses are required for failover of the WebLogic Server Administration Server, regardless of whether other Oracle Fusion Middleware components are installed later or not.

You associate the Administration Server and each of the Managed Servers with a virtual IP address. This allows the Administration Server to be started on a different host if the primary host fails.

Check that each virtual host is enabled as Table 6–3 shows.

Table 6–3   Virtual Hosts for the Domain

Virtual IP Address	Enabled on Host
ADMINVHN.example.com	WCCHOST1
WCCHOST1VHN1.example.com	WCCHOST1
WCCHOST2VHN1.example.com	WCCHOST2
WCCHOST1VHN2.example.com	WCCHOST1
WCCHOST2VHN2.example.com	WCCHOST2
WCCHOST1VHN3.example.com	WCCHOST1
WCCHOST2VHN3.example.com	WCCHOST2

> **Note:**   This is the DNS name associated with the floating IP address. It is not the DNS name of the virtual host configured on the load balancer.

6.6.2 Enabling Virtual IP Addresses for the Enterprise Deployment

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

You associate an Administration Server with a virtual IP address. This allows the Administration Server to be started on a different host if the primary host fails.

To enable a virtual IP address from a Linux system, run the following commands as root:

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

In the commands, *interface* is eth0 or eth1, and *index* is 0, 1, or 2.

For example:

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

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

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

Validate that the address is available by issuing the ping command from another node; for example:

```
/bin/ping 100.200.140.206
```

6.7 Configuring Users and Groups

Groups

You must create the following groups on each node.

- `oinstall`

- `dba`

Users

You must create the following users on each node.

- `oracle`: The group that owns the Oracle software. You may use a different name. The primary group for this account must be `oinstall`. The account must also be in the `dba` group.

- `nobody`: An unprivileged user.

> **Notes:**
>
> - The group `oinstall` must have the write privilege for all the file systems on shared and local storage that are used by the Oracle software.
>
> - Each group must have the same group ID on every node.
>
> - Each user must have the same user ID on every node.

7

Installing the Software for an Enterprise Deployment

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.

This chapter includes the following sections:

- Section 7.1, "Overview of the Software Installation Process"
- Section 7.2, "Installing Oracle HTTP Server"
- Section 7.3, "Installing Oracle Fusion Middleware"

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

7.1 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 components. Later chapters describe the required configuration steps to create the Oracle WebCenter Content reference topology.

Where to Obtain and Download 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.

What Software to Install

Table 7–1 shows what software should be installed on each host or be accessible from each host.

Table 7–1   Software To Be Installed on Each Host or Accessible from Each Host

Hosts	Oracle HTTP Server	Oracle WebLogic Server	Oracle WebCenter Content	Oracle SOA Suite	WebCenter Content User Interface
WEBHOST1	X				
WEBHOST2	X				
WCCHOST1		X	X	X	
WCCHOST2		X	X	X	
CSUIHOST1					X
CSUIHOST2					X

7.2 Installing Oracle HTTP Server

This section covers these topics:

- Section 7.2.1, "Prerequisites for Installing Oracle HTTP Server"
- Section 7.2.2, "Installing Oracle HTTP Server on WEBHOST1 and WEBHOST2"
- Section 7.2.3, "Backing Up the Installation"

7.2.1 Prerequisites for Installing Oracle HTTP Server

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

- Ensure that the system, patch, kernel, and other requirements are met as specified in the *Oracle Fusion Middleware Installation Guide for Oracle Web Tier*.

- Because Oracle HTTP Server is installed on port 7777 by default, you must make sure that port 7777 is not used by any service on the nodes. To check if this port is in use, run the following command before installing Oracle HTTP Server:

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

  You must free port 7777 if it is in use.

- On Linux platforms, if the `/etc/oraInst.loc` file exists, check that its contents are correct. Specifically, check that the inventory 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

7.2.2 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. Follow the same procedure to install Oracle HTTP Server on WEBHOST1 and on WEBHOST2.

To install Oracle HTTP Server on WEBHOST1 and WEBHOST2:

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

    ```
    ./runInstaller
    ```

2. On the Specify Inventory Directory screen, perform the following steps:

    a. Enter `/u02/oracle/oraInventory` on the local private storage volume mounted on each server node.

    b. Enter the OS group for the user performing the installation.

    c. Click **Next**.

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

    Click **OK**.

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

4. On the Install Software Updates screen, choose **Skip Software Updates** and click **Next**.

5. On the Select Installation Type screen, select **Install Software - Do Not Configure**, and click **Next**.

6. On the Prerequisite Checks screen, verify that all checks complete successfully, and click **Next**.

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

    - **Oracle Middleware Home** (installation location):
      `/u02/oracle/products/fmw_home`

    - **Oracle Home Directory:** `web_home`

    Click **Next**.

8. On the Specify Security Updates screen, choose whether you want to receive security updates from Oracle support and if you do, enter your email address.

9. On 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. On the Installation Completed screen, click **Finish** to exit.

11. Validate the installation by verifying that the following directories appear in the Middleware home directory after you install Oracle HTTP Server:

    - `oracle_common`

    - `web_home`

7.2.3 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 /u02/oracle/products/fmw_home /u02/oracle/oraInventory
```

7.3 Installing Oracle Fusion Middleware

This section describes how to install Oracle Fusion Middleware software in a Middleware home (*MW_HOME*) for the Oracle WebCenter Content enterprise deployment reference topology. The software components to be installed include Oracle JRockit, Oracle WebLogic Server, in the WebLogic Server home (*WL_HOME*), Oracle WebCenter Content, in the WebCenter Content Oracle home (*WCC_ORACLE_HOME*), and, optionally, Oracle SOA Suite, in the SOA Oracle home (*SOA_ORACLE_HOME*). As described in Chapter 4, "Preparing the File System for an Enterprise Deployment," you install Oracle Fusion Middleware in at least two storage locations for redundancy.

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

This section covers these topics:

- Section 7.3.1, "Creating a Middleware Home Directory"
- Section 7.3.2, "Installing Oracle JRockit in a Middleware Home"
- Section 7.3.3, "Installing Oracle WebLogic Server"
- Section 7.3.4, "Installing Oracle Fusion Middleware Components"
- Section 7.3.5, "Backing Up the Installation"

7.3.1 Creating a Middleware Home Directory

The Middleware home is where you can install Oracle Fusion Middleware products. The Middleware home (*MW_HOME*) contains the WebLogic Server home (*WL_HOME*), the Oracle Common home (*ORACLE_COMMON_HOME*), and, optionally, the JDK home (*JAVA_HOME*) and one or more Oracle homes for Oracle Fusion Middleware components and products, including Oracle WebCenter Content (*WCC_ORACLE_HOME*).

A Middleware home can reside on a local file system or on a remote shared disk that is accessible through Network File System (NFS).

Before you install the Oracle Fusion Middleware software, you need to create a Middleware home directory, as follows:

```
mkdir /u01/oracle/products/fmw_home/
```

7.3.2 Installing Oracle JRockit in a Middleware Home

To install Oracle JRockit in a Middleware home:

1. Download the version of Oracle JRockit for your platform from the Oracle Technology Network:

   ```
   http://www.oracle.com/technetwork/middleware/jrockit/downloads/index.html
   ```

2. Add execute permissions to Oracle JRockit. For example:

   ```
   chmod +x jrockit-1.6.0_29-R28.2.0-4.0.1-linux-x64.bin
   ```

3. Start the Oracle JRockit installer by issuing this command:

   ```
   ./jrockit-version.bin
   ```

   For example

   ```
   ./jrockit-1.6.0_29-R28.2.0-4.0.1-linux-x64.bin
   ```

4. On the Welcome Screen, click **Next**.

5. On the Choose Product Installation Directories screen, enter a **Product Installation Directory** value. This is the *JAVA_HOME* value, the path to a directory where Oracle JRockit will be installed inside your Middleware home. For example:

   ```
   /u01/oracle/products/fmw_home/JRockit_version
   ```

6. On the Optional Components Screen, click **Next**.

7. On the Installation Complete screen, click **Done**.

7.3.3 Installing Oracle WebLogic Server

Follow the same procedure to install Oracle WebLogic Server on WCCHOST1 and on WCCHOST2.

To install Oracle WebLogic Server on WCCHOST1 or WCCHOST2:

1. To install Oracle WebLogic Server on WCCHOST1 and WCCHOST2 on a 64-bit UNIX operating system, use either of these commands:

   ```
   JAVA_HOME/bin/java -jar wls103n_generic.jar

   JAVA_HOME/bin/java -d64 -jar wls103n_generic.jar
   ```

   To install Oracle WebLogic Server on WCCHOST1 and WCCHOST2 on a 32-bit UNIX operating system, start the installer for Oracle WebLogic Server like this:

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

2. On the Specify Inventory Directory screen, perform the following steps:

   a. Enter /u02/oracle/oraInventory on the local private storage volume mounted on each server node (this is the recommended location).

   b. Enter the OS group for the user performing the installation.

   c. Click **Next**.

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

   Click **OK**.

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

4. On the Choose Middleware Home Directory screen, perform the following steps:

   - Select **Create a new Middleware Home**.

   - For **Middleware Home Directory**, enter /u01/oracle/products/fmw_home.

     For more information, see Section 4.4, "Recommended Locations for Different Directories."

   Click **Next**.

5. On the Register for Security Updates screen, enter your contact information so that you can be notified of security updates, and click **Next**.

6. On the Choose Install Type screen, select **Custom**, and click **Next**.

7. On the Choose Products and Components screen, click **Next**.

8. On the JDK Selection screen, select **Oracle JRockit 1.6.0_*version* SDK**, and click **Next**.

> **Note:** The examples documented in this guide use Oracle JRockit. Any certified version of Java can be used for this procedure and is fully supported unless otherwise noted.

9. On the Choose Product Installation Directories screen, accept the directories *ORACLE_BASE***/product/fmw_home/wlserver_10.3** and *ORACLE_BASE***/product/fmw_home/coherence_3.7**, and click **Next**.

10. On the Installation Summary screen, click **Next**.

    The Oracle WebLogic Server software is installed.

11. On the Installation Complete screen, clear the **Run Quickstart** checkbox, and click **Done**.

12. 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-jdk1.6.0_version`
    - `modules`
    - `registry.xml`
    - `utils`
    - `domain-registry.xml`
    - `logs`
    - `ocm.rsp`
    - `registry.dat`
    - `wlserver_10.3`

7.3.4 Installing Oracle Fusion Middleware Components

This section covers these topics:

- Section 7.3.4.1, "Installing Oracle WebCenter Content"
- Section 7.3.4.2, "Installing Oracle SOA Suite"

7.3.4.1 Installing Oracle WebCenter Content

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

- Oracle WebCenter Content (WebCenter Content, which includes Oracle WebCenter Content Server)

- Oracle WebCenter Content: Inbound Refinery

- Oracle WebCenter Content: Imaging (which includes the Imaging Viewer Cache and AXF for BPEL)

- Oracle WebCenter Content: AXF for BPM

- Oracle WebCenter Enterprise Capture

- Oracle Information Rights Management (Oracle IRM)

- Oracle WebCenter Content: Records

To install Oracle WebCenter Content on WCCHOST1 and WCCHOST2:

1. Start the installer for Oracle WebCenter Content:

   ```
   wcc_media_loc/Disk1/runInstaller –jreLoc jre_location
   ```

   If you do not specify the JRE location, the installer either prompts you for the location or returns an error. If you get an error, retry the command with the JRE location included; for example, *MW_HOME*/jrockit-jdk1.6.0_*version*. For more information, see Section 7.3.3, "Installing Oracle WebLogic Server."

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

3. On the Install Software Updates screen, select **Skip Software Updates**, and click **Next**.

4. On the Prerequisite Checks screen, verify that all checks complete successfully, and click **Next**.

5. On the Specify Installation Location screen (Figure 7–1), provide the installation location for Oracle WebCenter Content. Select the previously installed Middleware home from the drop-down list. For the Oracle home directory, enter the directory name (wcc_home).

   Click **Next** when you are done.

Figure 7–1   Specify Installation Location Screen in the Installation Wizard
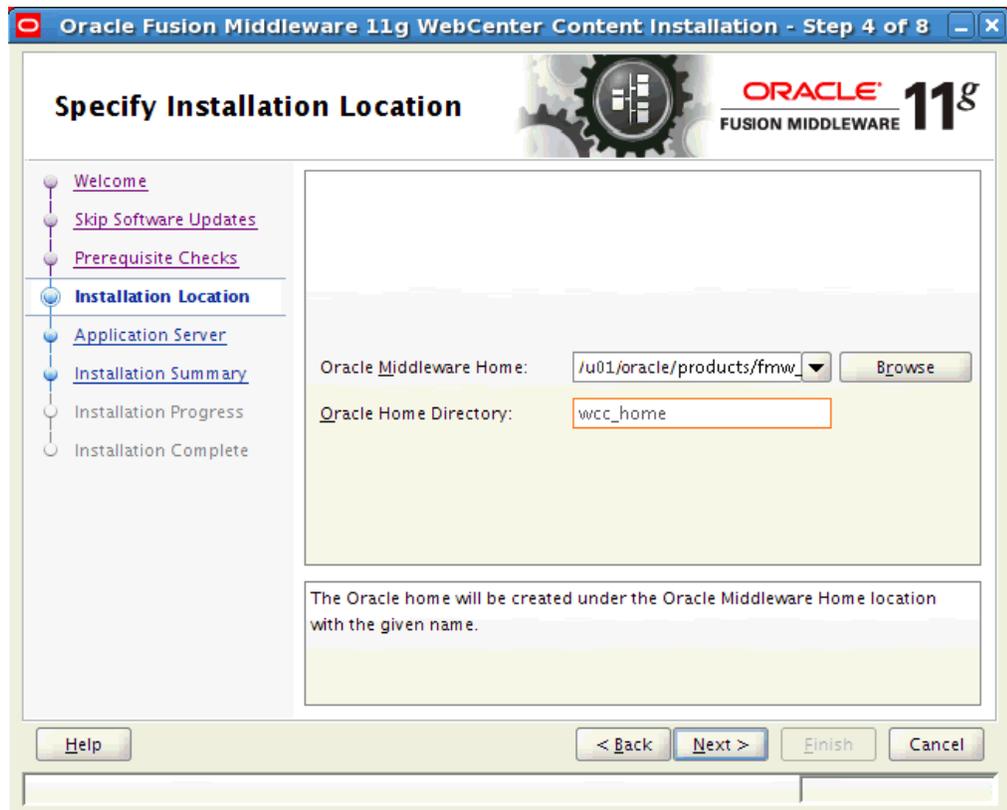
6. On the Application Server screen, make sure **WebLogic Server** is selected (which is the default), and click **Next**.

7. On the Installation Summary screen, click **Install**. The Oracle WebCenter Content software is installed.

8. On 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, and Oracle WebCenter Content:

    ■   coherence_*version*

    ■   jrockit-jdk*version*

    ■   modules

    ■   oracle_common

    ■   registry.xml

    ■   utils

    ■   domain-registry.xml

    ■   logs

    ■   ocm.rsp

    ■   registry.dat

    ■   wlserver_10.3

    ■   wcc

7.3.4.2 Installing Oracle SOA Suite

If you plan to use Oracle SOA Suite with Imaging, such as for the Oracle Application Extension Framework (AXF), you need to install and configure Oracle SOA Suite first. This section describes how to install it. For configuration information, see Section 12.3, "Extending the Domain for Oracle SOA Suite Components."

To install Oracle SOA Suite on WCCHOST1 and WCCHOST2:

1. On Linux platforms, if the `/etc/oraInst.loc` file exists, check that its contents are correct. Specifically, check that the inventory directory (`oraInventory`) 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:

   ```
   soa_media_loc/Disk1/runInstaller -jreLoc jre_location
   ```

   If you do not specify the JRE location, the installer either prompts you for the location or returns an error. If you get an error, retry the command with the JRE location included; for example, `MW_HOME/jrockit-jdk1.6.0_version`. For more information, see Section 7.3.3, "Installing Oracle WebLogic Server."

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

4. On the Install Software Updates screen, select **Skip Software Updates**, and click **Next**.

5. On the Prerequisite Checks screen, verify that all checks complete successfully, and click **Next**.

6. On the Specify Installation Location screen (Figure 7–1), provide the installation location for Oracle SOA Suite. Select the previously installed Middleware home from the drop-down list. For the Oracle home directory, enter the directory name (`soa`).

   Click **Next** when you are done.

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

8. On the Installation Summary screen, click **Install**.

   The Oracle SOA Suite software is installed.

9. On the Installation Complete screen, click **Finish**.

10. 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 WebCenter Content, 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`

- `wcc`

7.3.5 Backing Up the Installation

The Middleware home should be backed up now from WCCHOST1 (make sure that you stop the servers first):

```
tar -cvpf fmwhomeback.tar MW_HOME
```

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

8

Creating a Domain for an Enterprise Deployment

This chapter describes how to create a domain using the Fusion Middleware Configuration Wizard, Oracle WebLogic Server Administration Console, and Oracle Enterprise Manager Fusion Middleware Control. You can extend the domain to add Oracle Fusion Middleware components: Oracle SOA Suite, Oracle WebCenter Content and, optionally, Oracle WebCenter Content: Imaging and Oracle WebCenter Content: Inbound Refinery. Later chapters describe how to extend the domain.

This chapter includes the following sections:

- Section 8.1, "Overview of Creating a Domain"
- Section 8.2, "Enabling VIP1 on WCCHOST1"
- Section 8.3, "Running the Configuration Wizard on WCCHOST1 to Create a Domain"
- Section 8.4, "Performing Postconfiguration and Verification Tasks for the Domain"
- Section 8.5, "Reassociating the Domain with an OPSS Security Store in Oracle Database"
- Section 8.6, "Verifying Manual Failover of the Administration Server"
- Section 8.7, "Backing Up the WebLogic Server Domain Configuration"

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

8.1 Overview of Creating a Domain

Table 8–1 lists the steps for creating an Oracle WebLogic Server domain, including postconfiguration tasks.

Table 8–1   Steps for Creating a WebLogic Server Domain

Step	Description	More Information
Enabling VIP1 on WCCHOST1	Enable ADMINVHN for the WCCHOST1 host	Section 8.2, "Enabling VIP1 on WCCHOST1"
Create a WebLogic Server Domain	Run the Configuration Wizard to create a WebLogic Server domain.	Section 8.3, "Running the Configuration Wizard on WCCHOST1 to Create a Domain"
Perform postconfiguration and Verification Tasks	Follow the instructions for postconfiguration and validation tasks.	Section 8.4, "Performing Postconfiguration and Verification Tasks for the Domain"
Reassociate the File-Based Security Store with an OPSS Database-Based Security Store	Reassociate the default, file-based policy and credential store with an Oracle Platform and Security Services (OPSS) security store in Oracle Database 11.2.01 or later.	Section 8.5, "Reassociating the Domain with an OPSS Security Store in Oracle Database"
Verify Administration Server Failover	Test the manual failover of the Administration Server from WCCHOST1 to WCCHOST2.	Section 8.6, "Verifying Manual Failover of the Administration Server"
Back Up the Domain	Back up the newly configured WebLogic Server domain.	Section 8.7, "Backing Up the WebLogic Server Domain Configuration"

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

8.2 Enabling VIP1 on WCCHOST1

This step is required for failover of the Administration Server, regardless of whether or not other Oracle 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 virtual IP address (VIP1) by either a DNS Server or an entry in the custom /etc/hosts file. Check that ADMINVHN is available according to your name resolution system (DNS server or /etc/hosts) in the required nodes in your Oracle WebCenter Content topology. The virtual IP address (VIP1) that is associated to this Virtual Host Name (ADMINVHN) must be enabled on WCCHOST1.

Check that the virtual hosts are enabled as Table 8–2 shows. To enable the virtual IP address, see Section 6.6, "Enabling Virtual IP Addresses."

Table 8–2   Virtual Hosts for the Domain

Virtual IP Address	Enabled on Host
ADMINVHN.example.com	WCCHOST1
WCCHOST1VHN1.example.com	WCCHOST1
WCCHOST2VHN1.example.com	WCCHOST2
WCCHOST1VHN2.example.com	WCCHOST1
WCCHOST2VHN2.example.com	WCCHOST2
WCCHOST1VHN3.example.com	WCCHOST1
WCCHOST2VHN3.example.com	WCCHOST2

> **Note:** This is the DNS name associated with the floating IP address. It is not the DNS name of the virtual host configured on the load balancer.

8.3 Running the Configuration Wizard on WCCHOST1 to Create a Domain

Run the 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.

To run the Configuration Wizard on WCCHOST1 to create a domain:

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 WCCHOST1, change the directory to the location of the Fusion Middleware Configuration Wizard (created in Chapter 7, "Installing the Software for an Enterprise Deployment"):

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

   In the reference topology, `ORACLE_COMMON_HOME` is the `/u01/oracle/products/fmw_home/oracle_common` directory.

3. Start the Configuration Wizard:

   ```
   ./config.sh
   ```

4. On 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
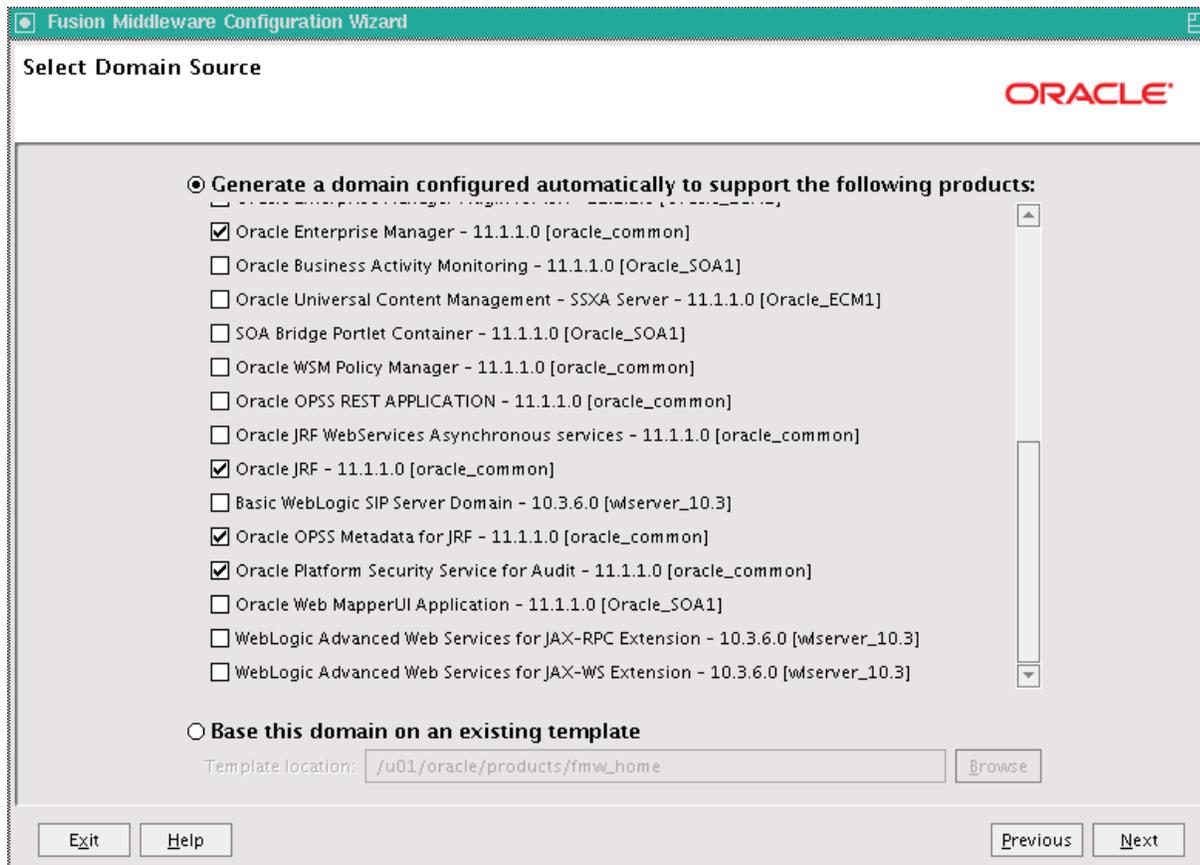
On the Select Domain Source screen, perform the following steps:

a.   Select **Generate a domain configured automatically to support the following products**.

b.   Select the following products:

–   **Basic WebLogic Server Domain** (this should be selected automatically)

–   **Oracle Enterprise Manager**

–   **Oracle JRF** (selected automatically)

–   **Oracle OPSS Metadata for JRF**

–   **Oracle Platform Security Services for Audit**

c.   Click **Next**.

6.   On the Specify Domain Name and Location screen, enter the name of the new domain, such as `WCCDomain`, and the domain and applications directories:

■   **Domain name:** `WCCDomain`

■   **Domain location:** `/u01/oracle/config/domains`

■   **Application location:** `/u01/oracle/config/applications`

The Configuration Wizard adds a subdirectory with the domain name to the domain location, to make the `ASERVER_HOME` directory, and to the application location, to make the `APPLICATION_HOME` directory.

Make sure that these directories match the directory and shared-storage mount points recommended in Chapter 4, "Preparing the File System for an Enterprise Deployment." The Managed Server domain directory for Oracle WebCenter Content should be under the local volume for each server.

Click **Next**.

7. On 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. On the Configure Server Start Mode and JDK screen, perform the following steps:

- For WebLogic Domain Startup Mode, select **Production Mode**.

- For JDK Selection, select **JROCKIT SDK1.6.0_*version***.

Note: The examples documented in this guide use Oracle JRockit. Any certified version of Java can be used for this procedure and is fully supported unless otherwise noted.

Click **Next**.

9. On the Configure JDBC Component Schema screen (Figure 8–2), perform the following steps:

a. Select these schemas:

* **OPSS Schema**

* **OPSS Audit Schema**

* **OPSS Audit Viewer Schema**

Figure 8–2   Configure JDBC Component Schema Screen for OPSS
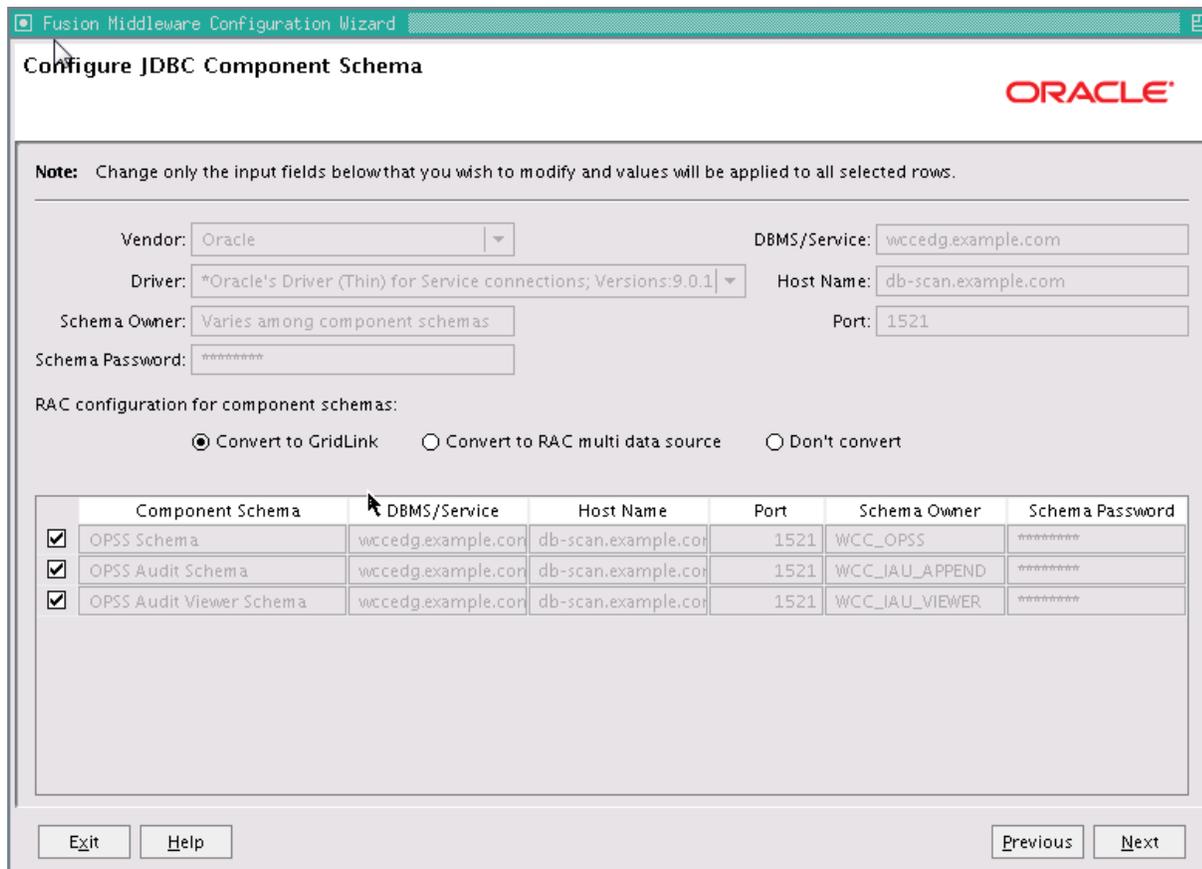
b. For the RAC configuration, you can select **Convert to GridLink** or **Convert to RAC multi data source** (described in Appendix A, "Using Multi Data Sources with Oracle RAC"). For the instructions given here, select **Convert to GridLink**.

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

c. Click **Next**.

10. On the Configure GridLink RAC Component Schema screen (Figure 8–3), perform the following steps:

a. Make sure all three schema rows are selected.

Figure 8–3   Configure GridLink RAC Component Schema Screen for OPSS

b. Enter values for the following fields, specifying the connection information for the GridLink RAC database that was seeded through RCU:

–   **Driver:** Select **Oracle's river (Thin) for GridLink Connections; Versions: 11 and later**.

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

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

This book uses `WCC` 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`.

Creating a Domain for an Enterprise Deployment   **8-7**

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>show parameter remote_listener;

NAME               TYPE        VALUE
-----              ------      -------
remote_listener    string      db-scan.example.com:1521
```

> **Note:** For Oracle Database 11*g*, use the virtual IP address and port of each database instance listener, as in these examples:
>
> ```
> wccdbhost1-vip.example.com (port 1521)
>
> wccdbhost2-vip.example.com (1521)
> ```
>
> 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@WCCDBHOST2~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016
```

> **Note:** For Oracle Database 11*g*, use the host name and port of each database's ONS service, as in these examples:
>
> ```
> wccdbhost1.example.com (port 6200)
>
> wccdbhost2.example.com (6200)
> ```

c. Click **Next**.

11. On the Test JDBC Component Schema screen (Figure 8–4), select all three schema rows, 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 8–4   Test JDBC Component Schema Screen for OPSS
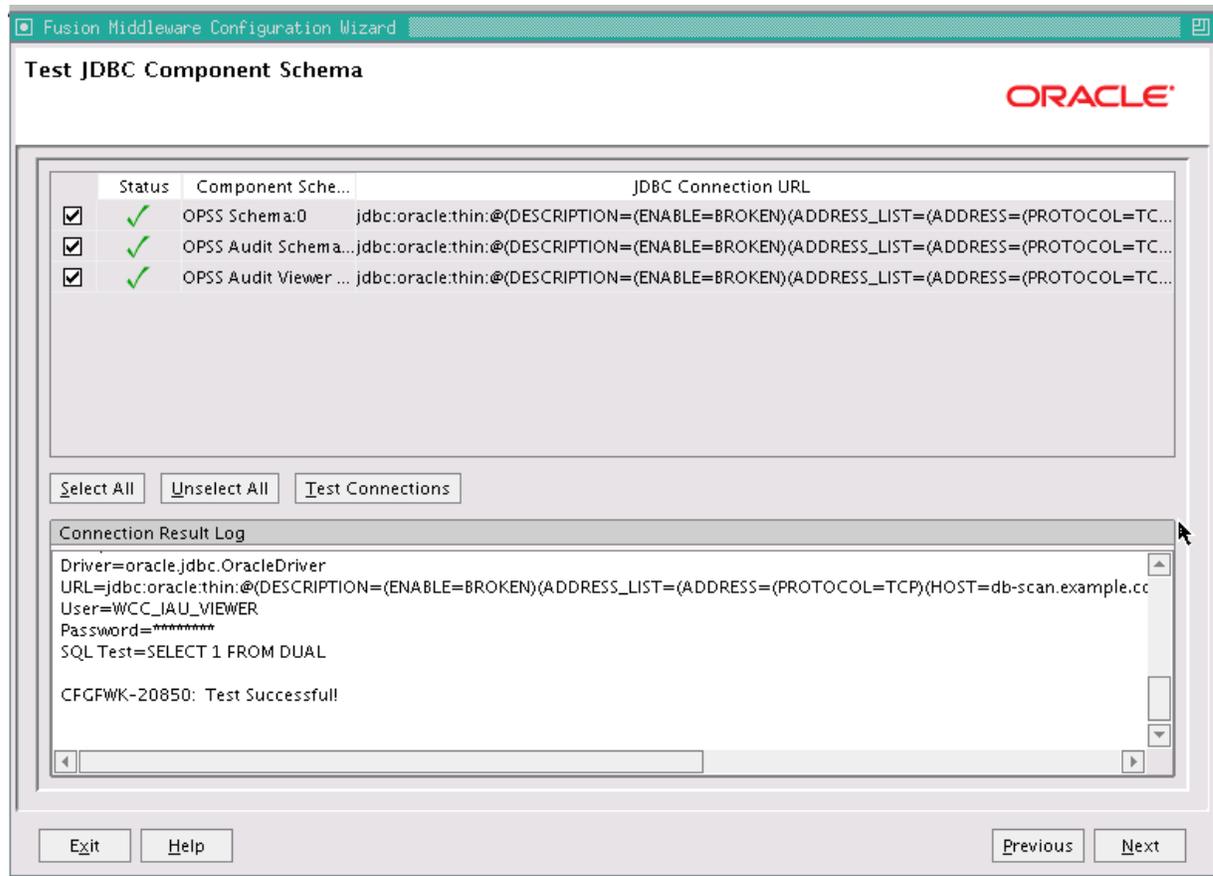
Click **Next** when the connection is successful.

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

   ■ **Administration Server**

   ■ **Managed Servers, Clusters and Machines**

   Click **Next**.

13. On 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**.

14. On the Configure Managed Servers screen, click **Next**.

15. On the Configure Clusters screen, click **Next**.

16. On the Configure Machines screen, open the **Unix Machine** tab and then click **Add** to add the following machine.

Table 8–3   Machine for the Administration Server

Name	Node Manager Listen Address
ADMINHOST	localhost

Leave all other fields set to their default values. 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.

> **Note:**   The Node Manager listen address for ADMINHOST must point to `localhost` because `localhost` is the relative internal address for whatever machine is active. The Node Manager instance associated with the Administration Server changes when the Administration Server fails over because the Administration Server uses the `localhost` attribute in conjunction with the first host and then again, after failover, in conjunction with the second host.

Click **Next**.

17. On the Assign Servers to Machines screen, assign the Administration Server to a machine as follows:

- **ADMINHOST:**

    – AdminServer

Click **Next**.

18. On the Configuration Summary screen, click **Create**.

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

8.4 Performing Postconfiguration and Verification Tasks for the Domain

After configuring the domain with the Configuration Wizard, follow these instructions for postconfiguration and verification.

The section includes the following topics:

- Section 8.4.1, "Creating boot.properties for the Administration Server on WCCHOST1"

- Section 8.4.2, "Starting Node Manager on WCCHOST1"

- Section 8.4.3, "Starting the Administration Server on WCCHOST1"

- Section 8.4.4, "Validating the Administration Server Configuration"

- Section 8.4.5, "Disabling Host Name Verification"

- Section 8.4.6, "Copying the Domain Registry File to the Middleware Home on WCCHOST2"

8.4.1 Creating boot.properties for the Administration Server on WCCHOST1

Create a `boot.properties` file for the Administration Server on WCCHOST1. This file enables the Administration Server to start without prompting you for the administrator user name and password.

To create a `boot.properties` file for the Administration Server on WCCHOST1:

1. Create the following directory structure on WCCHOST1:

   ```
   mkdir -p ASERVER_HOME/servers/AdminServer/security
   ```

   In the reference topology, *ASERVER_HOME* is the
   `/u01/oracle/config/domains/WCCDomain` directory.

2. In a text editor, create a file called `boot.properties` in the directory created in the previous step, and enter the following lines into the file:

   ```
   username=admin_user
   password=admin_password
   ```

   The values of *admin_user* and *admin_password*, are the user name and password of the WebLogic Server domain administrator.

   > **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 8.4.3, "Starting the Administration Server on WCCHOST1." For security reasons, you want to minimize the time the entries in the file are left unencrypted. After you edit the file, you should start the server as soon as possible so that the entries get encrypted.

3. Save the file, and close the editor.

8.4.2 Starting Node Manager on WCCHOST1

To start Node Manager on WCCHOST1, set the `StartScriptEnabled` property to `true`, and then start Node Manager using `startNodeManager.sh`.

To start Node Manager on WCCHOST1:

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

   ```
   cd ORACLE_COMMON_HOME/common/bin

   ./setNMProps.sh
   File nodemanager.properties not found. Copying required properties file.
   ```

   In the reference topology, *ORACLE_COMMON_HOME* is the `/u01/oracle/products/fmw_home/oracle_common` directory.

2. Start Node Manager:

   ```
   cd WL_HOME/server/bin

   export JAVA_OPTIONS=-DDomainRegistrationEnabled=true

   nohup ./startNodeManager.sh > nm.out&
   ```

   In the reference topology, *WL_HOME* is the `/u01/oracle/products/fmw_home/wlserver_10.3` directory.

> **Note:** It is important to set the `-DDomainRegistrationEnabled=true` parameter whenever Node Manager is started, to manage the Administration Server. If there is no Administration Server on the machine and the machine is not an Administration Server failover node, then you can start Node Manager with the following script (without the `export` command).
>
> ```
> nohup ./startNodeManager.sh > nm.out&
> ```

8.4.3 Starting the Administration Server on WCCHOST1

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 Fusion Middleware Configuration Wizard set for Node Manager. You must therefore use the start script for the Administration Server for the first start. In the following procedure, steps 1 through 4 are required for the first start; all subsequent starts require only step 4.

To start the Administration Server on WCCHOST1:

1. On WCCHOST1, start the Administration Server using the start script in the domain directory:

   ```
   cd ASERVER_HOME/bin
   ```

   ```
   ./startWebLogic.sh
   ```

   In the reference topology, `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

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

   a. Open a web browser and go to `http://ADMINVHN:7001/console`.

   b. Log in as `weblogic`.

   c. Click **Lock & Edit**.

   d. Click *domain_name*, then **Security**, and then **General**, and 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 WebLogic Server Administration Server by issuing the command `stopWebLogic.sh` located under the `ASERVER_HOME/bin` directory.

   Alternatively, you can 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
   ```

In the reference topology, *ORACLE_COMMON_HOME* is the `/u01/oracle/products/fmw_home/oracle_common` directory.

Once in the WLST shell, execute the following commands (make sure Node Manager is up and running):

```
wls:/offline>nmConnect("node_admin_user","node_admin_password",
"WCCHOST1","5556", "domain_name","ASERVER_HOME")

wls:/nm/domain_name> nmStart("AdminServer")
```

> **Notes:**
>
> - WCCHOST1 is the address of the node where the domain was created, not the listen address of the Administration Server.
>
> - The values of *node_admin_user* and *node_admin_password* are the Node Manager credentials that were updated in Step 2e. Independent from the server administrator ID and password, the Node Manager administrator user name and password are used only to authenticate connections between Node Manager and clients. These credentials are stored in the *ASERVER_HOME*/config/nodemanager/nm_password.properties file.

8.4.4 Validating the Administration Server Configuration

To ensure that the Administration Server for the domain you have created is properly configured, validate the configuration by logging in to the WebLogic Server Administration Console and verifying the Administration Server 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 8.4.1, "Creating boot.properties for the Administration Server on WCCHOST1."

The Administration Server should be up and running.

8.4.5 Disabling Host Name Verification

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server (see Chapter 16, "Setting Up Node Manager for an Enterprise Deployment"). If you have not configured the server certificates, you will receive errors when managing the different WebLogic Server instances. To avoid these errors, disable host name verification for the Administration Server and each Managed Server while setting up and validating the topology, and enable it again once the enterprise deployment topology configuration is complete, as described in Chapter 16, "Setting Up Node Manager for an Enterprise Deployment."

You can disable host name verification for a server as soon as it is up and running, starting with the Administration Server.

To disable host name verification:

1. Log in to the WebLogic Server Administration Console.

2. Click **Lock & Edit**.

3. In the **Domain Structure** tree on the left, expand the **Environment** node.

4. Click **Servers**.

5. On the Summary of Servers page, click the name of the Administration Server in the **Names** column of the **Servers** table.

6. On the settings page for the server, click the **SSL** tab.

7. Expand the **Advanced** section of the page.

8. Set **Hostname Verification** to None.

9. Click **Save**.

10. Save and activate the changes.

11. This change requires a restart of Node Manager and the Administration Server:

   a. Stop the Administration Server with Node Manager, using the following command:

   ```
   wls:/nm/domain_name>nmKill("AdminServer")
   ```

   b. Stop Node Manager by stopping the process associated with it.

   If it is running in the foreground in a shell, use Ctrl+C.

   If it is running in the background in the shell, find the associated 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
   ```

   c. Start Node Manager:

   ```
   cd WL_HOME/server/bin
   nohup ./startNodeManager.sh > nm.out&
   ```

   In the reference topology, `WL_HOME` is the `/u01/oracle/products/fmw_home/wlserver_10.3` directory.

   d. Start the Administration Server again, as follows:

   * Start the Oracle WebLogic Scripting Tool (WLST):

   ```
   cd ORACLE_COMMON_HOME/common/bin

   ./wlst.sh
   ```

   In the reference topology, `ORACLE_COMMON_HOME` is the `/u01/oracle/products/fmw_home/oracle_common` directory.

     * In the WLST shell, connect to Node Manager with the `nmConnect` command and the Node Manager credentials (make sure Node Manager is up and running), and start Node Manager and the Administration Server using `nmStart`:

```
wls:/offline>nmConnect("node_admin_user","node_admin_password",
"WCCHOST1","5556", "domain_name","ASERVER_HOME")
```

```
wls:/nm/domain_name> nmStart("AdminServer")
```

The values of *node_admin_user* and *node_admin_password* are the Node Manager credentials. For more information about the credentials, see Section 8.4.3, "Starting the Administration Server on WCCHOST1."

In the reference topology, *ASERVER_HOME* is the `/u01/oracle/config/domains/WCCDomain` directory.

8.4.6 Copying the Domain Registry File to the Middleware Home on WCCHOST2

As explained in Chapter 4, "Preparing the File System for an Enterprise Deployment," the Middleware home on WCCHOST2 is on a separate storage volume (local to WCCHOST2) to provide maximum redundancy for the installation binaries volume. The `domain-registry.xml` file created on WCCHOST1 during creation of the Administration Server domain is not created on WCCHOST2. You need to copy this file from WCCHOST1.

To copy the domain registry file from the Middleware home on WCCHOST1 to the Middleware home on WCCHOST2:

1. Go to the Middleware home directory on WCCHOST1.

```
cd MW_HOME
```

In the reference topology, `MW_HOME` is the `/u01/oracle/products/fmw_home` directory.

2. Copy the `domain-registry.xml` file to the Middleware home on WCCHOST2, with the following command:

```
scp domain-registry.xml oracle@WCCHOST2:MW_HOME/
```

3. Copy the `nodemanger.domains` file from WCCHOST1 to WCCHOST2, with the following command:

```
scp WL_HOME/common/nodemanager/nodemanager.domains oracle@WCCHOST2:WL_
HOME/common/nodemanager/
```

In the reference topology, *WL_HOME* is the `/u01/oracle/products/fmw_home/wlserver_10.3` directory.

8.5 Reassociating the Domain with an OPSS Security Store in Oracle Database

An OPSS security store is the repository of system and application-specific policies, credentials, and keys. This centralization facilitates the administration and maintenance of policy, credential, and key data. Oracle Fusion Middleware allows using different types of security stores for an Oracle WebLogic Server domain. A domain can use a security store based on an XML file (the default), Oracle Database, or Oracle Internet Directory.

For the enterprise deployment topology, a centralized security store is required for policies, credentials, and keys. Oracle recommends that you reassociate the security store for your Oracle WebCenter Content domain with an OPSS security store in Oracle Database 11*g* Release 2 (11.2).

Reassociating the OPSS security store consists of relocating the policy, credential, and key stores from one repository to another one. Reassociation changes the repository, preserving the integrity of the data stored. For each security artifact, reassociation searches the target store and if it finds a match, updates the matching artifact; otherwise, it creates a new artifact.

The source can be file-based, database-based, or LDAP-based (through a Lightweight Directory Application Protocol provider). The target can be database-based or LDAP-based. The only type of LDAP target supported is Oracle Internet Directory, and the only type of database target supported is Oracle Database 11.2.0.1 or later. For more information about using Oracle Internet Directory, see Section 18.2, "Reassociating the Identity Store with an External LDAP Authentication Provider."

For this operation, You can use either Oracle Enterprise Manager Fusion Middleware Control or the Oracle WebLogic Scripting Tool (WLST) `reassociateSecurityStore` command, as the following instructions describe.

8.5.1 Preparing to Reassociate the Domain with a Database-Based OPSS Security Store

Before you reassociate the OPSS security store, you need to back up your configuration files, verify that the OPSS schema was created correctly, and create an OPSS data source.

8.5.1.1 Backing Up Configuration Files

To be safe, before you change the OPSS security store, you should back up the relevant configuration files:

1. Back up the domain configuration files:

   ```
   ASERVER_HOME/WCCDomain/config/config.xml
   ASERVER_HOME/WCCDomain/config/fmwconfig/jps-config.xml
   ASERVER_HOME/WCCDomain/config/fmwconfig/system-jazn-data.xml
   ```

   In the reference topology, `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

2. Back up the `boot.properties` file for the Administration Server:

   ```
   ASERVER_HOME/servers/AdminServer/security/boot.properties
   ```

8.5.1.2 Verifying the OPSS Schema in Oracle Database

Before you reassociate the OPSS security store, you need to verify that the OPSS schema was created in Oracle Database by the Repository Creation Utility (RCU), as described in Section 5.4, "Creating Database Schemas."

To verify the OPSS schema in Oracle Database:

1. Log in to SQL*Plus:

```
ORACLE_HOME/bin/sqlplus sys/password as SYSDBA

SQL>
```

In the reference topology, *ORACLE_HOME* is the `/u01/oracle/products/fmw_home/wcc_home` directory.

2. Invoke the following SQL*Plus command to verify that the database schema has been properly created:

```
SQL>desc WCC_OPSS.jps_dn;
 Name Null? Type
 --------------------------------------- --------
 --------------------------
 ENTRYID NOT NULL NUMBER
 RDN NOT NULL VARCHAR2(1024)
 PARENTDN NOT NULL VARCHAR2(1024)

SQL>
```

8.5.2 Reassociating the File-Based OPSS Security Store with a Database-Based OPSS Security Store

To reassociate the domain's default, file-based OPSS security store with a database-based OPSS security store:

1. From WCCHOST1, start the `wlst` shell:

```
cd ORACLE_COMMON_HOME/common/bin

./wlst.sh
```

In the reference topology, *ORACLE_COMMON_HOME* is the `/u01/oracle/products/fmw_home/oracle_common` directory.

2. Connect to the WebLogic Server Administration Server using the following `wlst` `connect` command.

Syntax:

```
connect("admin_user","admin_password","t3://hostname:port")
```

For example:

```
wls:/offline> connect ("weblogic","welcome1","t3://ADMINVHN:7001")
Connecting to t3://ADMINVHN:7001 with userid weblogic ...
Successfully connected to Admin Server 'AdminServer' that belongs to domain
'WCCDomain'.

Warning: An insecure protocol was used to connect to the
server. To ensure on-the-wire security, the SSL port or
Admin port should be used instead.
```

3. Run the `reassociateSecurityStore` command, as follows:

Syntax:

```
reassociateSecurityStore(domain="domain_name",servertype="DB_
ORACLE",datasourcename="opss_datasource_name", jpsroot="cn=jpsroot_wcc")
```

For example:

```
wls:/WCCDomain/serverConfig>

reassociateSecurityStore(domain="WCCDomain",servertype="DB_
ORACLE",datasourcename="jdbc/OPSSDBDS", jpsroot="cn=jpsroot_wcc")
```

Output from the command follows:

```
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.
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store. Check logs for any failures or warnings during
migration.
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Policy store reassociation done.
Starting credential store reassociation
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store. Check logs for any failures or warnings during
migration.
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Credential store reassociation done
Starting Keystore reassociation
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store. Check logs for any failures or warnings during
migration.
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Keystore reassociation done
Starting audit store reassociation
The store and ServiceConfigurator setup done.
Schema is seeded into the store
Data is migrated to the store. Check logs for any failures or warnings during
migration.
Data in the store after migration has been tested to be available
Update of in-memory jps configuration is done
Audit store reassociation done
Jps Configuration has been changed. Please restart the application server.
wls:/WCCDomain/serverConfig>
```

4. Restart the Administration Server after the command completes successfully, as follows:

   a. Start the Oracle WebLogic Scripting Tool (WLST):

      ```
      cd ORACLE_COMMON_HOME/common/bin

      ./wlst.sh
      ```

   b. Stop the Administration Server, using either the Administration Console or, as follows, the Node Manager nmKill command:

      ```
      wls:/nm/domain_name>nmKill("AdminServer")
      ```

    c. Start the Administration Server using `nmstart`:

```
wls:/nm/domain_name> nmStart("AdminServer")
```

> **Note:** The Administration Server log will contain some OPSSS audit warning messages that are benign, and you can safely ignore them.

5. Validate the reassociation of the security store:

    a. Log in to Oracle Enterprise Manager Fusion Middleware Control for the new domain, at this URL (in the reference topology):

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

    b. Expand **WebLogic Domain**, and click **WCCDomain**.

    c. From the **WebLogic Domain** menu on the WCCDomain page, choose **Security** and then **Security Provider Configuration**.

    d. In the **Security Stores** table on the Security Provider Configuration page, verify that the value in the **Store Type** column is **Oracle Database**, as Figure 8–5 shows.

Figure 8–5   Oracle Database Security Provider
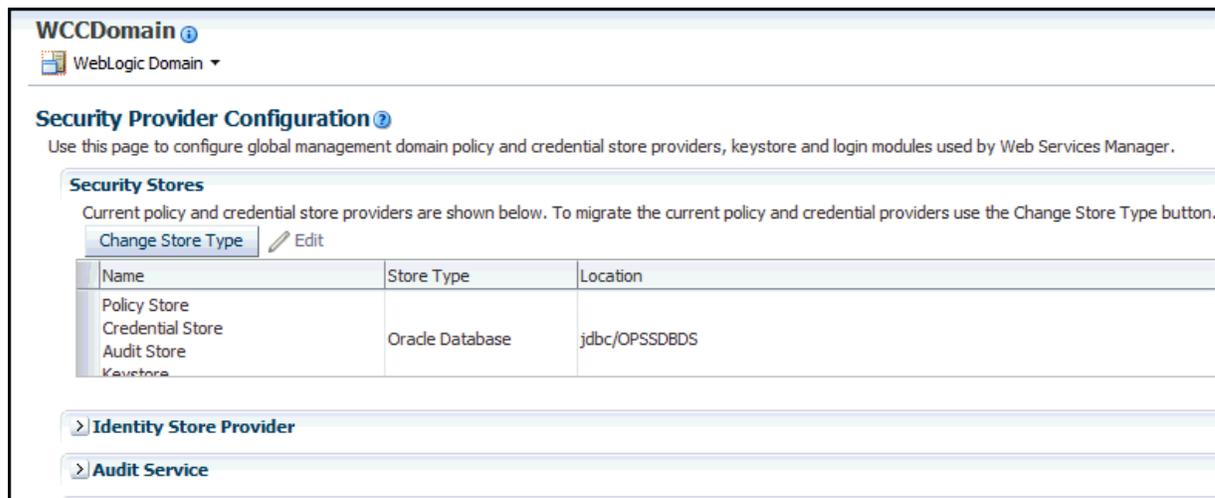
8.6 Verifying Manual Failover of the Administration Server

After configuring the domain, test failover by following the steps in Section 19.8, "Verifying Manual Failover of the Administration Server."

8.7 Backing Up the WebLogic Server Domain Configuration

After you have verified that the 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 with the steps for extending the domain in later chapters. 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 about backups. 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. For information about database backups, see the *Oracle Database Backup and Recovery User's Guide*.

To back up the installation and configuration at this point:

1. Stop the Administration Server and back up its domain directory to save your domain configuration. The configuration files all exist in the `ASERVER_HOME` directory. Run the following command on WCCHOST1 to create the backup:

   ```
   tar -cvpf edgdomainback.tar ASERVER_HOME
   ```

   In the reference topology, `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

   To stop the Administration Server, use the WLST `nmKill` command:

   a. Start the Oracle WebLogic Scripting Tool (WLST):

   ```
   cd ORACLE_COMMON_HOME/common/bin

   ./wlst.sh
   ```

   In the reference topology, `ORACLE_COMMON_HOME` is the `/u01/oracle/products/fmw_home/oracle_common` directory.

   b. In the WLST shell, connect to Node Manager with the `nmConnect` command and the Node Manager credentials (make sure Node Manager is up and running):

   ```
   wls:/offline>nmConnect("node_admin_user","node_admin_password",
   "WCCHOST1","5556", "domain_name","ASERVER_HOME")
   ```

   The values of `node_admin_user` and `node_admin_password` are the Node Manager credentials. For more information about the credentials, see Section 8.4.3, "Starting the Administration Server on WCCHOST1."

   c. Stop the Administration Server, using the `nmKill` command:

   ```
   wls:/nm/domain_name>nmKill("AdminServer")
   ```

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. Start the Administration Server using `nmstart`:

   ```
   wls:/nm/domain_name> nmStart("AdminServer")
   ```

9

Configuring Oracle Web Tier for an Enterprise Deployment

This chapter describes how to configure Oracle Web Tier to support the Oracle WebCenter Content implementation.

This chapter includes the following sections:

9.1 Overview of Configuring Oracle Web Tier

Before configuring the Oracle Web Tier software, you need to install it on WEBHOST1 and WEBHOST2, as described in Section 7.2, "Installing Oracle HTTP Server," and define the instance home, instance name, and Oracle HTTP Server component name, as described in Section 9.2, "Running the Configuration Wizard to Configure Oracle HTTP Server."

Then you can validate the installation and configure the load balancer to route all HTTP requests to WEBHOST1 and WEBHOST2.

Finally, you can configure the virtual hosts by defining directives in configuration files. You created the following virtual host names when you configured the load balancer in Section 3.3, "Load Balancers":

- `admin.example.com`
- `wcc.example.com`
- `wccinternal.example.com`

9.2 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 Oracle Web Tier:

1. Change the directory to the location of the Web Tier configuration wizard:

   ```
   cd WT_ORACLE_HOME/bin
   ```

   In the reference topology, *WT_ORACLE_HOME* is the `/u02/oracle/products/fmw_home/web_home` directory.

2. Start the configuration wizard:

   ```
   ./config.sh
   ```

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

4. On the Configure Components screen, select **Oracle HTTP Server**, and ensure that **Associate Selected Components with WebLogic Domain** is selected. Make sure that Oracle Web Cache is *not* selected.

   Click **Next**.

5. On the Specify WebLogic Domain screen, specify the following value:

   - **Domain Host Name:** `ADMINVHN`

   - **Domain Port No:** `7001`

   - **User Name:** `weblogic`

   - **Password:** *password*

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

   - **Instance Home Location**: /u02/oracle/config/web*n*

   - **Instance Name**: web*n*

   - **OHS Component Name**: ohs*n*

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

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

   Click **Next**.

7. On the Configure Ports screen, select **Specify Ports using Configuration file**, then select a file name, and then click **View/Edit**.

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

   The file will look like this:

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

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

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

Click **Next**.

8. On the Specify Security Updates screen, choose whether you want to receive security updates from Oracle support and if you do, enter your email address.

9. On 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**.

10. Multiple configuration assistants are launched in succession; this process can be lengthy. When it completes, click **Next**.

11. On the Installation Complete screen, click **Finish** to exit.

9.3 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.example.com:7777/
http://WEBHOST2.example.com:7777/
```

9.4 Configuring Oracle HTTP Server with the Load Balancer

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

9.5 Defining Virtual Hosts

The reference topology in this guide requires that you define a set of virtual hosts for the Oracle HTTP Server. For each virtual host, you will later define a set of specific URLs that will route requests to the proper Administration Server or Managed Server in the WebLogic Server domain.

This section contains the following topics:

- Section 9.5.1, "Creating *_vh.conf Files to Define <VirtualHost> Directives"
- Section 9.5.2, "Validating the Configuration"

9.5.1 Creating *_vh.conf Files to Define <VirtualHost> Directives

You need to define each virtual host in its own `*_vh.conf` file in every *ORACLE_INSTANCE*/ohs*n*/moduleconf directory. This will make it easy to manage the URLs for each virtual host you define.

You define the `<VirtualHost>` directives in the following new files:

- `admin_vh.conf`

- `wccinternal_vh.conf`

- `wcc_vh.conf`

- `wccui_vh.conf`

In the reference topology, you create these files in each of the following directories:

```
/u02/oracle/config/web1/config/OHS/ohs1/moduleconf
```

```
/u02/oracle/config/web2/config/OHS/ohs2/moduleconf
```

To define each virtual host in its own `*_vh.conf` file:

1. Create the `admin_vh.conf` file in the *ORACLE_INSTANCE*/ohs*n*/moduleconf directory, and add the following directive:

```
NameVirtualHost *:7777
<VirtualHost *:7777>
    ServerName admin.example.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit
    RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end_
url=/console" [R]
</VirtualHost>
```

   If the steps in Chapter 18, "Integrating with Oracle Identity Management," have not been completed, then comment out the `RewriteRule` lines until the integration has been completed.

2. Create the `wccinternal_vh.conf` file in the *ORACLE_INSTANCE*/ohs*n*/moduleconf directory, and add the following directive:

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

3. Create the `wcc_vh.conf` file in the *ORACLE_INSTANCE*/ohs*n*/moduleconf directory, and add the following directive:

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

4. Create the `wccui_vh.conf` file in the `ORACLE_INSTANCE`/ohs*n*/moduleconf directory, and add the following directive:

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

5. Restart both Oracle HTTP Servers:

```
cd /u02/oracle/config/webN/bin
opmnctl stopall
opmnctl startall
```

> **Note:** Values such as `wcc.example.com:443`, `ServerAdmin you@your.address`, and `admin.example.com:80` are only examples. Enter values based on your actual environment.

9.5.2 Validating the Configuration

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

- `http://admin.example.com/index.html`

- `https://wcc.example.com/index.html`

- `http://wccinternal.example.com/index.html`

If you cannot access these URLs, check to ensure that you correctly completed the procedure in Section 3.3, "Load Balancers."

9.6 Configuring Oracle HTTP Server for the WebLogic Server Domain

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

This section includes the following topics:

- Section 9.6.1, "Configuring Oracle HTTP Server for the Administration Server"

- Section 9.6.2, "Turning On the WebLogic Server Plug-In Enabled Flag"

- Section 9.6.3, "Setting the Front-End URL for the Administration Console and Setting Redirection Preferences"

- Section 9.6.4, "Validating Access Through the Load Balancer"

9.6.1 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.

To configure Oracle HTTP Server for the Administration Server:

1. For each of the web servers on WEBHOST1 and WEBHOST2, add the following lines to the *ORACLE_INSTANCE*/config/OHS/ohs1/moduleconf/admin_vh.conf and *ORACLE_INSTANCE*/config/OHS/ohs2/moduleconf/admin_vh.conf files:

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

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

```
/u02/oracle/config/webN/bin/opmnctl restartproc ias-component=ohsX
```

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

9.6.2 Turning On the WebLogic Server 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 you configure SSL for the load balancer, turn on the WebLogic Server plug-in enabled flag for the domain.

To turn on the WebLogic Server plug-in enabled flag:

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):

   a. Start the Oracle WebLogic Scripting Tool (WLST):

   ```
   cd ORACLE_COMMON_HOME/common/bin

   ./wlst.sh
   ```

   b. In the WLST shell, connect to Node Manager with the `nmConnect` command and the Node Manager credentials (make sure Node Manager is up and running), and start the Node Manager using `nmStart`:

   ```
   wls:/offline>nmConnect("node_admin_user","node_admin_password",
   "WCCHOST1","5556", "domain_name","ASERVER_HOME")

   wls:/nm/domain_name> nmStart("AdminServer")
   ```

   The values of *node_admin_user* and *node_admin_password* are the Node Manager credentials. For more information about the credentials, see Section 8.4.3, "Starting the Administration Server on WCCHOST1."

   In the reference topology, *ASERVER_HOME* is the `/u01/oracle/config/domains/WCCDomain` directory.

   c. Stop the Administration Server, using either the Administration Console or, as follows, the WLST `nmKill` command:

   ```
   wls:/nm/domain_name>nmKill("AdminServer")
   ```

   d. Start the Administration Server using `nmStart`:

   ```
   wls:/offline>nmConnect("node_admin_user","node_admin_password",
   "WCCHOST1","5556", "domain_name","ASERVER_HOME")

   wls:/nm/domain_name> nmStart("AdminServer")
   ```

9.6.3 Setting the Front-End URL for the Administration Console and Setting Redirection Preferences

When you access the WebLogic Server Administration Console using a load balancer, you must change the Administration Server's front-end 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 front-end URL:

1. Log in to the WebLogic Server Administration Console.

2. Click **Lock & Edit**.

3. Expand the **Environment** node in the **Domain Structure** tree on the left.

4. Click **Servers**.

5. On the Summary of Servers page, click **Admin Server** in the **Names** column of the table.

6. On the settings page for `AdminServer`, click the **Protocols** tab.

7. Click the **HTTP** tab.

8. Set the **Frontend Host** field to `admin.example.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. Restart the Administration Server for changes to the front-end host directive to take effect.

> **Note:** If you have any issues with activating any configuration changes after modifying the front-end host and port settings, see Section 19.13.10, "Redirection of Users to Administration Console's Home Page After Activating Changes to Oracle Access Manager."

9.6.4 Validating Access Through the Load Balancer

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. For possible causes, see Section 19.13, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology."

Validate access to the Administration Console and Oracle Enterprise Manager Fusion Middleware Control through the load balancer using the following URLs:

- `http://admin.example.com/console`
- `http://admin.example.com/em`

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

Oracle HTTP Server 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.

10

Extending the Domain to Include WebCenter Content

This chapter describes how to extend the domain created in Chapter 8, "Creating a Domain for an Enterprise Deployment," to include Oracle WebCenter Content, which includes Oracle WebCenter Content Server, using the Fusion Middleware Configuration Wizard. You can extend the resulting domain to add other Oracle Fusion Middleware components, as described in the following chapters.

This chapter includes the following sections:

- Section 10.1, "Overview of Extending the Domain to Include WebCenter Content"
- Section 10.2, "Extending the Domain for WebCenter Content"
- Section 10.3, "Restarting the Administration Server"
- Section 10.4, "Completing Postconfiguration and Verification Tasks for WebCenter Content"
- Section 10.5, "Configuring Content Server for the WebCenter Content User Interface"
- Section 10.6, "Configuring Oracle HTTP Server with the WebCenter Content Cluster"
- Section 10.7, "Configuring Node Manager for the WLS_WCC Managed Servers"
- Section 10.8, "Backing Up the Installation"

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

10.1 Overview of Extending the Domain to Include WebCenter Content

The Oracle WebCenter Content system is installed using the WebLogic Server home and Oracle home locations created in Chapter 7, "Installing the Software for an Enterprise Deployment," on a shared storage.

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 10–1   Steps for Extending the Domain with WebCenter Content

Step	Description	More Information
Extend the domain for WebCenter Content	Extend the WebLogic Server domain you created in Chapter 8, "Creating a Domain for an Enterprise Deployment," to include Oracle WebCenter Content.	Section 10.2, "Extending the Domain for WebCenter Content"
Start Node Manager on the WebCenter Content Managed Servers	Run the setNMProps.sh script and then start Node Manager on WCCHOST1 and on WCCHOST2.	Section 10.4.1, "Starting Node Manager on WCCHOST2"
Propagate the domain configuration to the WebCenter Content Managed Servers	Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the Managed Server domain directories.	Section 10.4.2, "Propagating the Domain Configuration to WLS_WCC1 and WLS_WCC2"
Restart the Administration Server for the domain	Stop and then restart the Administration Server.	Section 10.3, "Restarting the Administration Server"
Start the first WebCenter Content Managed Server and configure its Content Server instance	Start the WLS_WCC1 Managed Server and complete the initial Content Server configuration.	Section 10.4.3, "Starting the WLS_WCC1 Managed Server and Configuring Content Server"
Propagate the changes in the cwallet.sso file back to the Administration Server.	Copy the updated cwallet.sso file to the Administration Server directory.	Section 10.4.4, "Updating the cwallet File in the Administration Server"
Start the second WebCenter Content Managed Server and configure its Content Server instance	Configure the WLS_WCC2 Managed Server and complete the initial Content Server configuration.	Section 10.4.5, "Starting the WLS_WCC2 Managed Server and Configuring Content Server"
Verify the configuration of GridLink data sources and Oracle Notification Service (ONS)	Follow these instructions to verify that the configuration of GridLink data sources and ONS is correct.	Section 10.4.6, "Validating GridLink Data Sources for WebCenter Content"
Configure parameters for cluster nodes	Add directory locations for WebCenter Content trace and event logs, as needed.	Section 10.4.7, "Configuring Additional Parameters"
Enable service retries after an Oracle RAC failover	Set the ServiceAllowRetry configuration parameter to `true` in the Content Server `config.cfg` file.	Section 10.4.8, "Configuring Service Retries for Oracle WebCenter Content"
Configure Oracle HTTP Server with the extended domain	Configure the Oracle HTTP Server with the Managed Servers, set the front-end HTTP host and port, and set the WebLogic Server cluster address for WCC_Cluster.	Section 10.6, "Configuring Oracle HTTP Server with the WebCenter Content Cluster"
Validate access to WebCenter Content through Oracle HTTP Server	Verify the URLs to ensure that appropriate routing and failover is working from Oracle HTTP Server to WCC_Cluster.	Section 10.6.3, "Validating Access Through the Load Balancer"
Configure host name verification for communication between Node Manager and the Managed Servers in the domain	Use certificates for the different addresses communicating with the Administration Server and other servers.	Section 10.7, "Configuring Node Manager for the WLS_WCC Managed Servers"
Back Up the WebCenter Content Configuration	Back up the newly extended domain configuration.	Section 10.8, "Backing Up the Installation"

10.2 Extending the Domain for WebCenter Content

You can extend the domain created in Section 8, "Creating a Domain for an Enterprise Deployment" to include Oracle WebCenter Content.

> **Note:** Before performing these steps, back up the domain as described in the *Oracle Fusion Middleware Administrator's Guide*.

To extend the domain for 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 WCCHOST1, 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. On the Welcome screen, select **Extend an existing WebLogic domain**, and click **Next**.

5. On the Select a WebLogic Domain Directory screen, select the WebLogic Server domain directory (*ASERVER_HOME*), and click **Next**.

6. On 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

     This is the selection for Oracle WebCenter Content.

Figure 10–1 Select Extension Source Screen for WebCenter Content
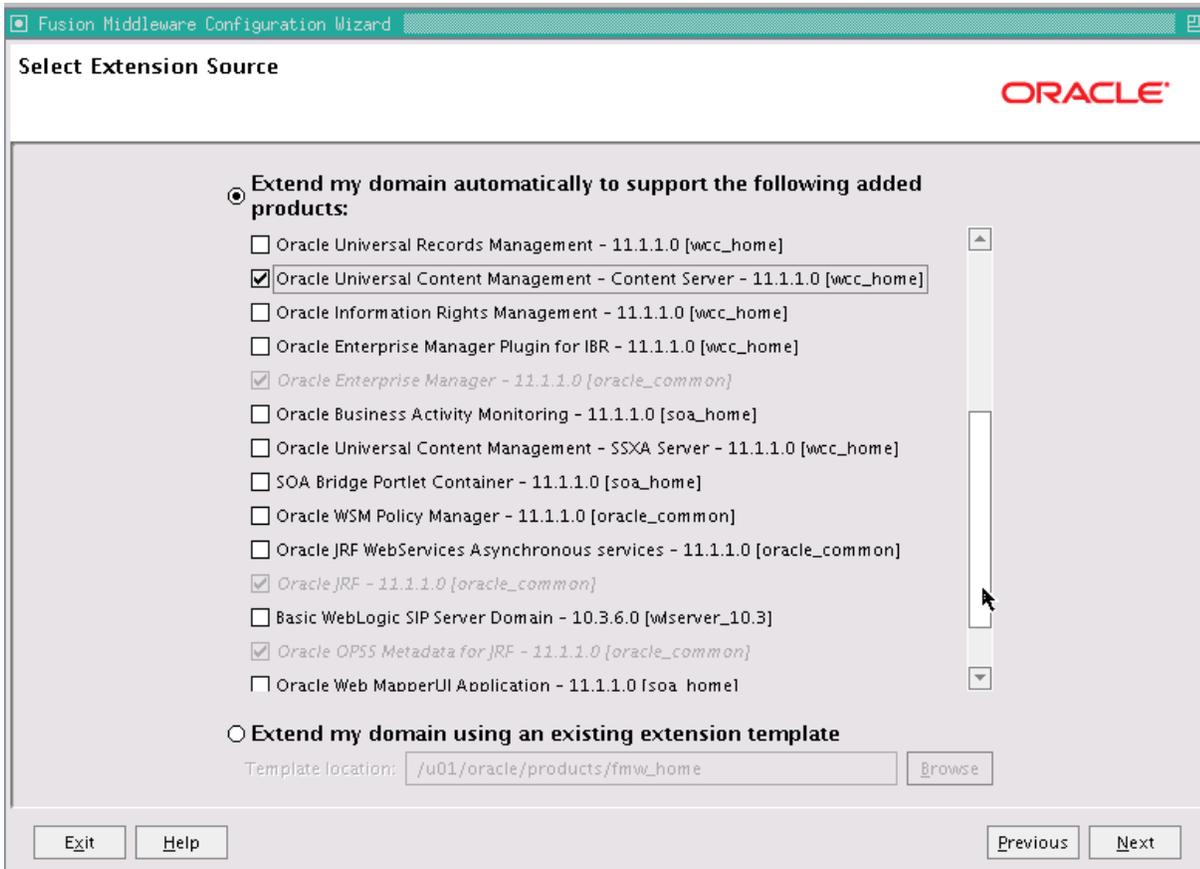
The following products are grayed out if they were selected when you created the domain (Section 8.3).

- **Basic WebLogic Server Domain**

- **Oracle Enterprise Manager**

- **Oracle JRF**

Click **Next**.

7. On the Configure JDBC Component Schema screen (Figure 10–2), perform the following steps:

   a. Select **UCM Schema** (for WebCenter Content).

Figure 10–2   Configure JDBC Component Schema Screen for WebCenter Content

    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. On the Configure GridLink RAC Component Schema screen (Figure 10–3), perform the following steps:

    a. Make sure **UCM Schema** is selected.

Figure 10–3   Configure GridLink RAC Component Schema Screen for WebCenter Content

b. Enter values for the following fields, specifying the connection information for the GridLink RAC database that was seeded through RCU:

–   **Driver:** Select **Oracle's Driver (Thin) for GridLinkConnections; Versions: 11 and later**.

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

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

    This book uses `WCC` 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>show parameter remote_listener;

NAME              TYPE        VALUE
-----             ------      -------
remote_listener   string      db-scan.example.com:1521
```

> **Note:** For Oracle Database 11*g*, use the virtual IP address and port of each database instance listener, as in these examples:
>
> ```
> wccdbhost1-vip.example.com (port 1521)
> ```
>
> ```
> wccdbhost2-vip.example.com (1521)
> ```
>
> 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@WCCDBHOST2~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016
```

> **Note:** For Oracle Database 11*g*, use the host name and port of each database's ONS service, as in these examples:
>
> ```
> wccdbhost1.example.com (port 6200)
> ```
>
> ```
> wccdbhost2.example.com (6200)
> ```

c.   Click **Next**.

9.   On 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.

Figure 10–4 Test JDBC Component Schema Screen for WebCenter Content
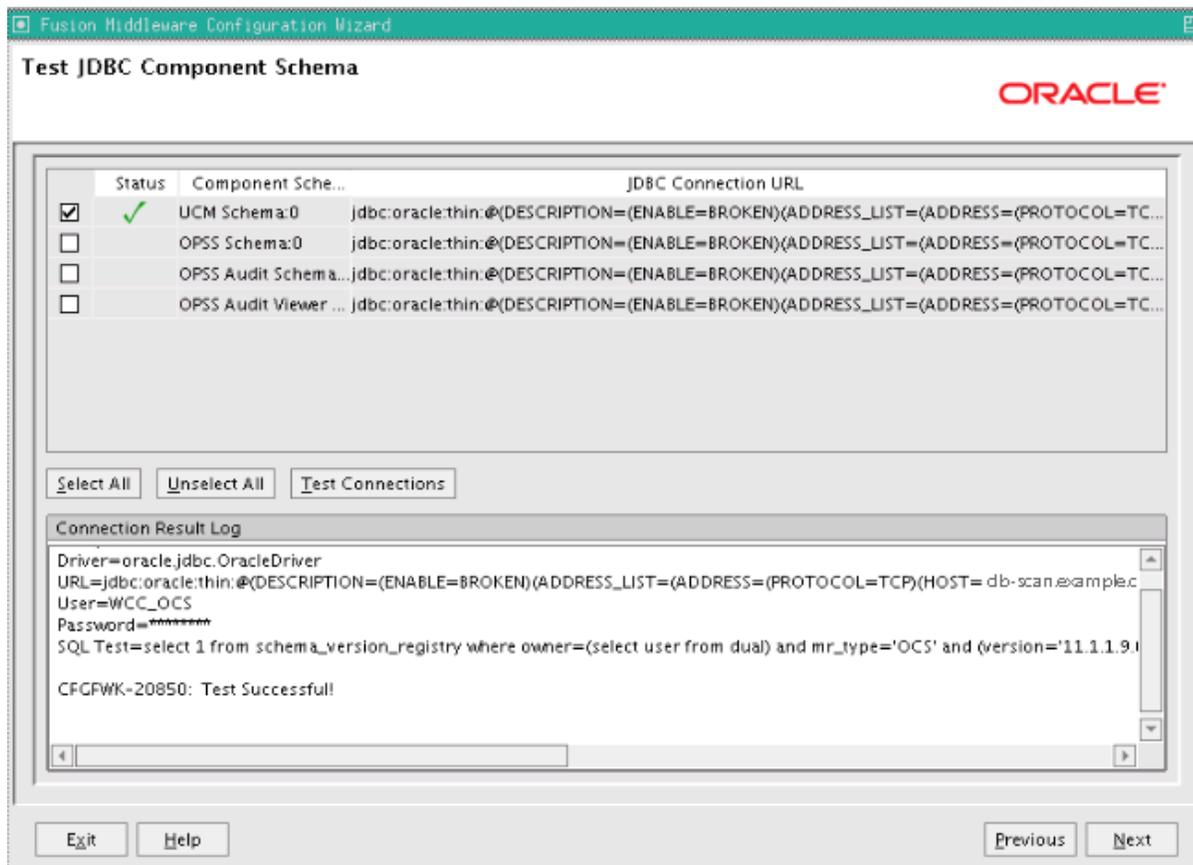
Click **Next** when the connection is successful.

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

   ■ **Managed Servers, Clusters and Machines**

   ■ **Deployment and Services**

   Click **Next**.

11. On the Configure Managed Servers screen (Figure 10–5), add the required Managed Servers.

Figure 10–5 Configure Managed Servers for WebCenter Content
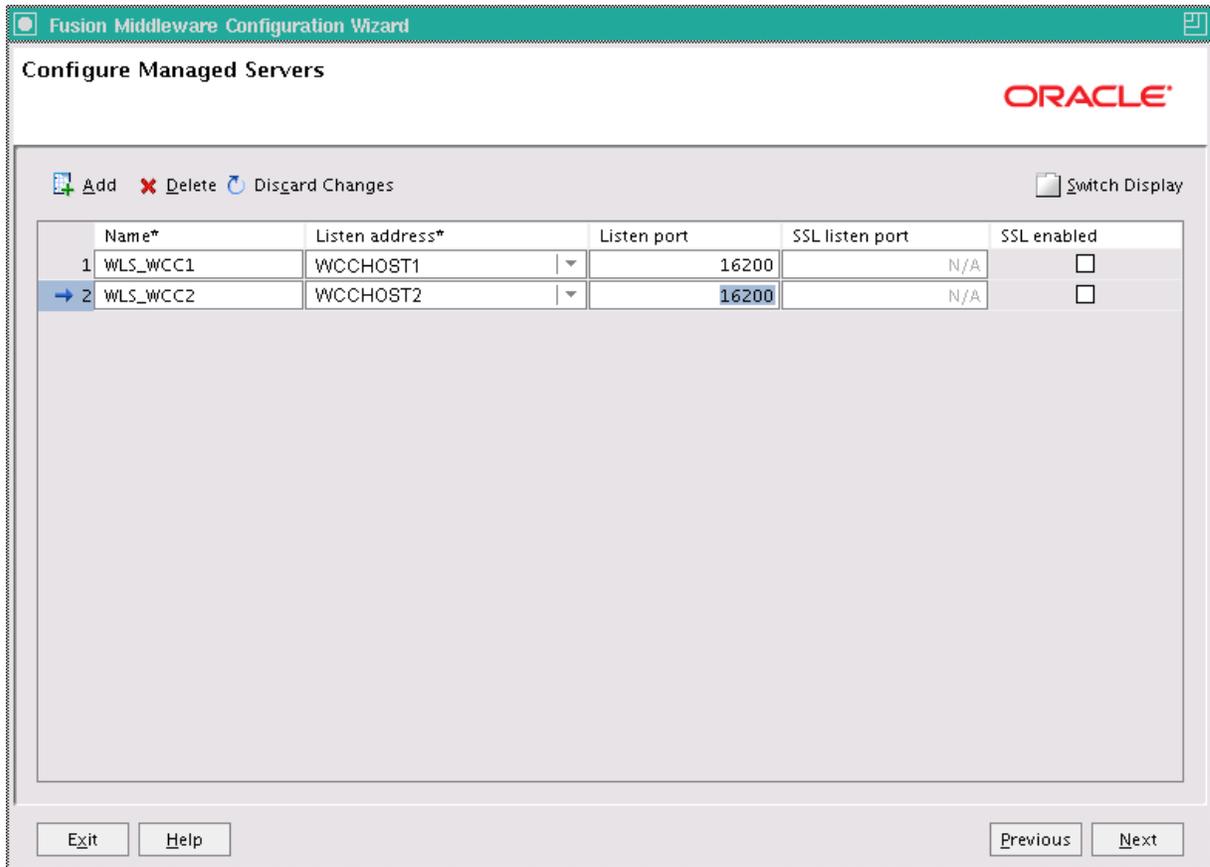
A server is created automatically. Rename this server to WLS_WCC1 and add a new server called WLS_WCC2. Give these servers the attributes listed in Table 10–2. Do not modify the other servers that are shown on this screen.

Table 10–2 Managed Servers for WebCenter Content

Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
WLS_WCC1	WCCHOST1	16200	n/a	No
WLS_WCC2	WCCHOST2	16200	n/a	No

Click **Next**.

12. On the Configure Clusters screen (Figure 10–6, click **Add** and enter WCC_Cluster, which Table 10–3 describes.

Table 10–3 Cluster Configuration for WebCenter Content

Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
WCC_Cluster	unicast	n/a	n/a	Leave empty.

Figure 10–6   Configure Clusters Screen for WebCenter Content
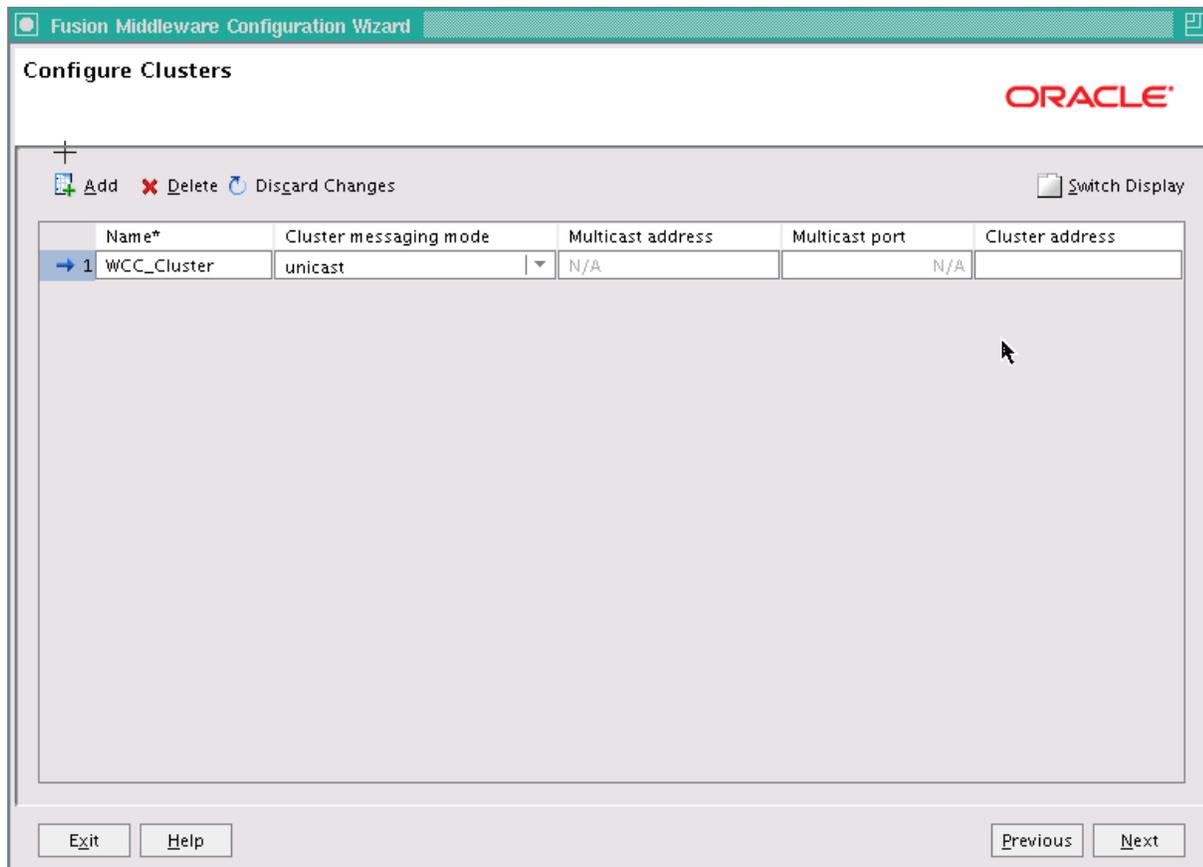
Click **Next**.

13. On the Assign Servers to Clusters screen, assign the following servers to **WCC_Cluster**:

    – `WLS_WCC1`

    – `WLS_WCC2`

    Click **Next**.

14. On the Configure Machines screen, open the **Unix Machine** tab, and add the following two machines.

Table 10–4   Machines for WebCenter Content

Name	Node Manager Listen Address
WCCHOST1	WCCHOST1
WCCHOST2	WCCHOST2
ADMINHOST	localhost

Leave all other fields set to their default values. 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**.

15. On the Assign Servers to Machines screen (Figure 10–7), assign servers to machines as follows:

- Assign **WLS_WCC1** to **WCCHOST1**.

- Assign **WLS_WCC2** to **WCCHOST2**.

Figure 10–7 Assign Servers to Machines Screen for WebCenter Content
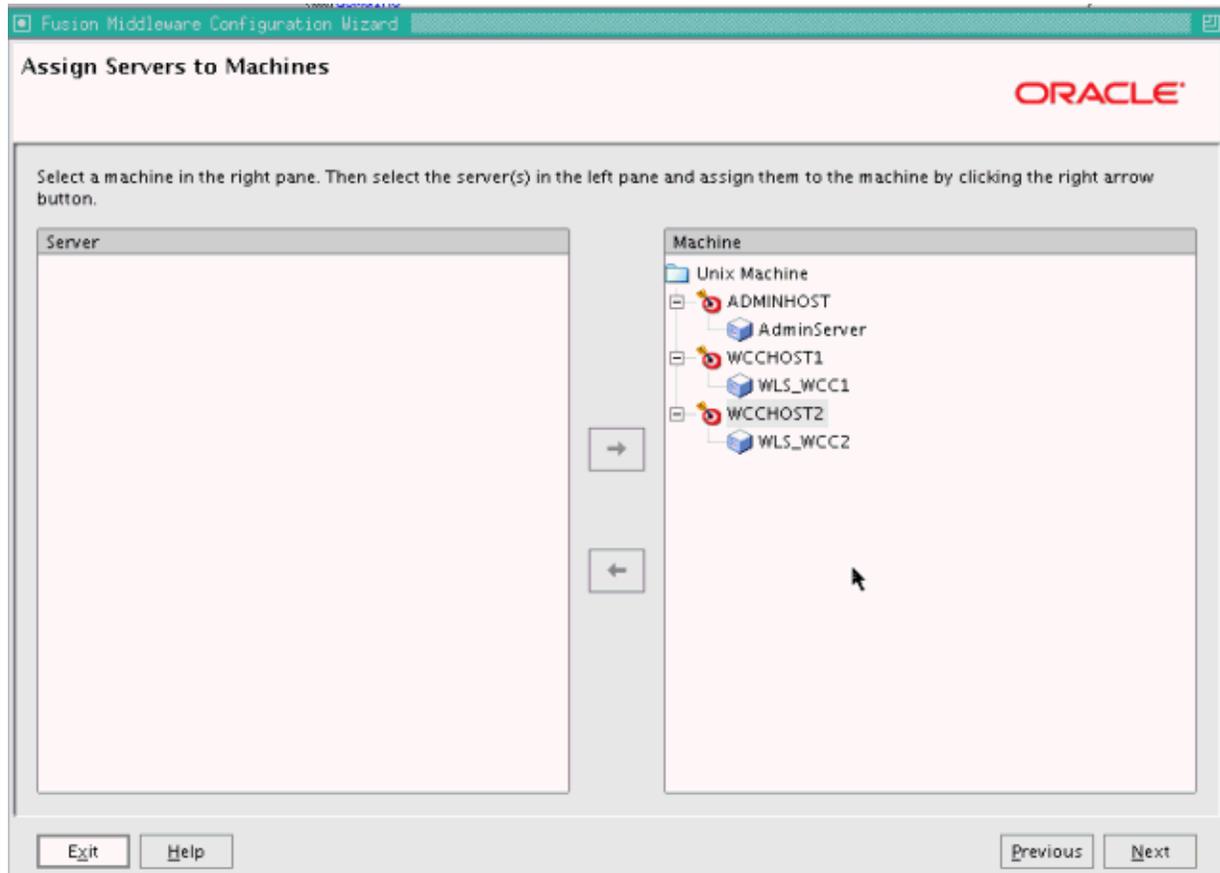
Click **Next**.

16. On the Target Deployments to Clusters or Servers screen, make sure that targeting is done as follows:

- **DMS Application** is targeted to **WCC_Cluster** and **AdminServer**.

- **EM Application** is targeted only to **AdminServer**.

Click **Next**.

17. On the Target Services to Clusters or Servers screen, select all OPSS-related data sources to be deployed to **WCC_Cluster**, as Figure 10–8 shows:

- **opss-audit-viewDS**

- **opss-audit-DBDS**

- **opss-DBDS**

Figure 10–8   Target Services to the WebCenter Content Cluster
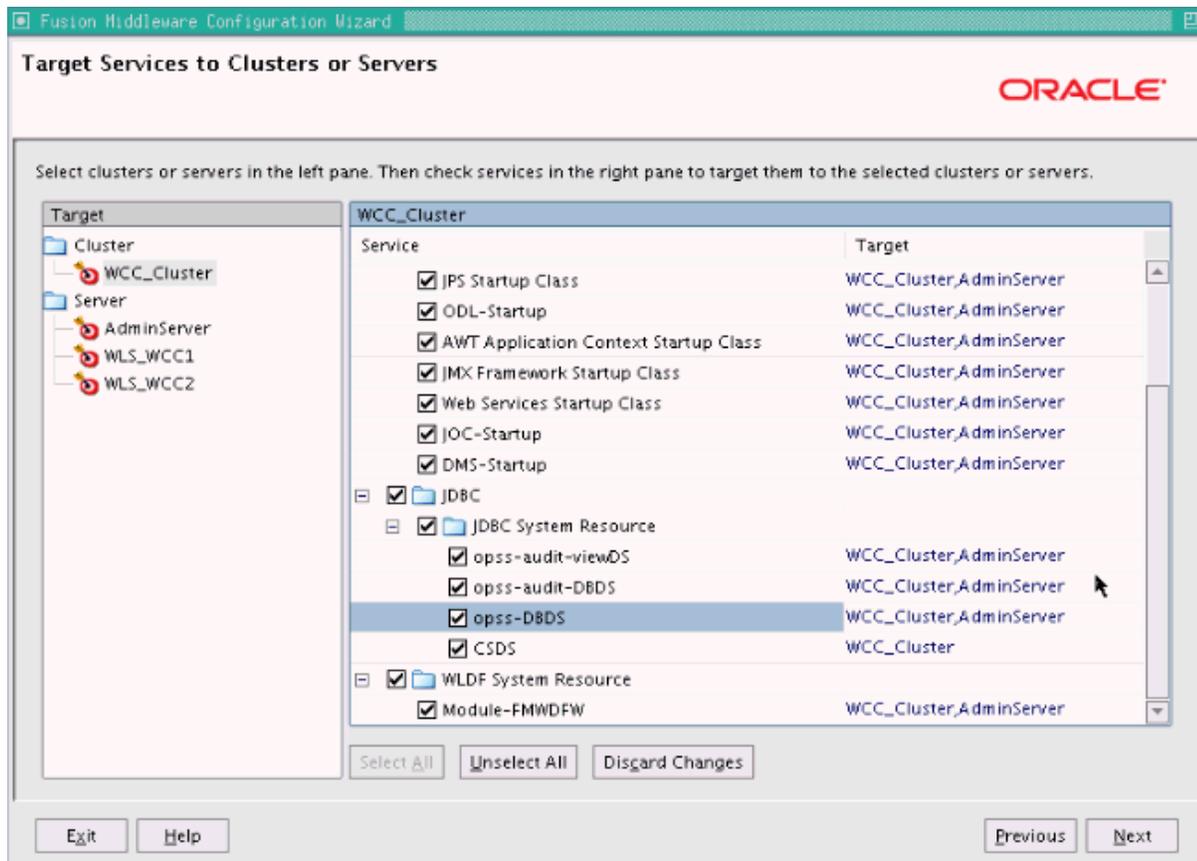
Click **Next**.

18. On the Configuration Summary screen, click **Extend**.

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

20. On the Creating Domain screen, click **Done**.

10.3 Restarting the Administration Server

You need to restart the Administration Server to make the domain extension changes take effect, using the Node Manager `nmKill` and `nmStart` commands through the Oracle WebLogic Scripting Tool (WLST). You can use the Administration Console instead of `nmKill` to stop the Administration Server. After the restart, log in to the Administration Console using the credentials for the `weblogic` user.

To restart the Administration Server:

1. Start the Oracle WebLogic Scripting Tool (WLST):

```
cd ORACLE_COMMON_HOME/common/bin

./wlst.sh
```

In the reference topology, *ORACLE_COMMON_HOME* is the `/u01/oracle/products/fmw_home/oracle_common` directory.

2. In the WLST shell, connect to Node Manager with the `nmConnect` command and the Node Manager credentials (make sure Node Manager is up and running), and start the Node Manager using `nmStart`:

```
wls:/offline>nmConnect("node_admin_user","node_admin_password",
"WCCHOST1","5556", "domain_name","MSERVER_HOME")

wls:/nm/domain_name> nmStart("AdminServer")
```

The values of *node_admin_user* and *node_admin_password* are the Node Manager credentials. For more information about the credentials, see Section 8.4.3, "Starting the Administration Server on WCCHOST1."

In the reference topology, *MSERVER_HOME* is the `/u02/oracle/config/domains/WCCDomain` directory.

3. Stop the Administration Server, using either the Administration Console or, as follows, the Node Manager `nmKill` command:

```
wls:/nm/domain_name>nmKill("AdminServer")
```

4. Start the Administration Server using `nmStart`:

```
wls:/offline>nmConnect("node_admin_user","node_admin_password",
"WCCHOST1","5556", "domain_name","ASERVER_HOME")

wls:/nm/domain_name> nmStart("AdminServer")
```

In the reference topology, *ASERVER_HOME* is the `/u01/oracle/config/domains/WCCDomain` directory.

10.4 Completing Postconfiguration and Verification Tasks for WebCenter Content

The following sections describe how to do postconfiguration and verifications tasks for WebCenter Content:

- Section 10.4.1, "Starting Node Manager on WCCHOST2"

- Section 10.4.2, "Propagating the Domain Configuration to WLS_WCC1 and WLS_WCC2"

- Section 10.4.3, "Starting the WLS_WCC1 Managed Server and Configuring Content Server"

- Section 10.4.4, "Updating the cwallet File in the Administration Server"

- Section 10.4.5, "Starting the WLS_WCC2 Managed Server and Configuring Content Server"

- Section 10.4.6, "Validating GridLink Data Sources for WebCenter Content"

- Section 10.4.7, "Configuring Additional Parameters"

- Section 10.4.8, "Configuring Service Retries for Oracle WebCenter Content"

10.4.1 Starting Node Manager on WCCHOST2

If Node Manager has not started already on WCCHOST2, you need to start it.

To start Node Manager on WCCHOST2:

1. On 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
   ```

   In the reference topology, *ORACLE_COMMON_HOME* is the /u01/oracle/products/fmw_home/oracle_common directory.

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

   ```
   cd WL_HOME/server/bin

   nohup ./startNodeManager.sh > nm.out&
   ```

   In the reference topology, *WL_HOME* is the /u01/oracle/products/fmw_home/wlserver_10.3 directory.

10.4.2 Propagating the Domain Configuration to WLS_WCC1 and WLS_WCC2

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

To propagate the domain configuration to the WebCenter Content Managed Servers:

1. Create a copy of the Managed Server domain directory and the Managed Server applications directory.

2. Run the following pack command on WCCHOST1 to create a template pack:

   ```
   cd ORACLE_COMMON_HOME/common/bin

   ./pack.sh –managed=true –domain= ASERVER_HOME
   –template=edgdomaintemplateWCC.jar –template_name=edgdomain_templateWCC
   ```

   In the reference topology, *ORACLE_COMMON_HOME* is the /u01/oracle/products/fmw_home/oracle_common directory, and *ASERVER_HOME* is the /u01/oracle/config/domains/WCCDomain directory.

3. Run the following unpack command on WCCHOST1 to propagate the template created in the preceding step to the WLS_WCC1 domain directory:

   ```
   cd ORACLE_COMMON_HOME/common/bin

   ./unpack.sh –domain= MSERVER_HOME –template=edgdomaintemplateWCC.jar –app_dir=
   APPLICATION_HOME –overwrite_domain=true
   ```

   In the reference topology, *MSERVER_HOME* is the /u02/oracle/config/domains/WCCDomain directory, and *APPLICATION_HOME* is the /u01/oracle/config/applications/WCCDomain directory.

> **Notes:**
>
> - The configuration steps provided for this enterprise deployment topology are documented with the assumption that a local (per node) domain directory is used for each Managed Server.
>
> - The configuration steps provided in this enterprise deployment topology are documented with the assumption that a local (per node) domain directory is used for each Managed Server.
>
> - Make sure to run `unpack` from the *ORACLE_COMMON_HOME*`/common/bin` directory, not from *WL_HOME*`/common/bin`.
>
> - The *APPLICATION_HOME* directory gets backed up with this `unpack` command.
>
> - *APPLICATION_HOME* is shared by the Application Server and Managed Server for which the option `-overwrite_domain=true` is used in the `unpack` command.
>
> - 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.

4. Run the following command on WCCHOST1 to copy the template pack created in step 1 to WCCHOST2:

```
scp edgdomaintemplateWCC.jar oracle@WCCHOST2:ORACLE_COMMON_HOME/common/bin
```

5. Run the following `unpack` command on WCCHOST2 to unpack the propagated template to the WLS_WCC2 Managed Server domain directory:

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

```
./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateWCC.jar -app_
dir=APPLICATION_HOME
```

> **Notes:**
>
> - Make sure to run `unpack` from the *ORACLE_COMMON_HOME*`/common/bin` directory, not from *WL_HOME*`/common/bin`.
>
> - The *APPLICATION_HOME* directory gets backed up with this `unpack` command.

6. Restart the Administration Server to make these changes take effect, stopping it with the `nmKill` command, or with the Administration Console, and then starting it with the `nmStart` command, as described in Section 10.3, "Restarting the Administration Server." After the restart, log in to the Administration Server using the credentials for the `weblogic` user.

10.4.3 Starting the WLS_WCC1 Managed Server and Configuring Content Server

After you start the WLS_WCC1 Managed Server, you can configure Content Server through the web interface.

To start the WLS_WCC1 Managed Server:

1. Log in to the Oracle WebLogic Server Administration Console at `http://admin.example.com:7001/console`.

2. Start the WLS_WCC1 Managed Server through the Administration Console, as follows:

   a. Expand the **Environment** node in the **Domain Structure** tree on the left.

   b. Click **Servers**.

   c. On the Summary of Servers page, click the **Control** tab.

   d. Select **WLS_WCC1** from the **Servers** column of the table.

   e. Click **Start**.

3. 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. For possible causes, see Section 19.13, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology."

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 the `ASERVER_HOME`/WCC_Cluster directory.
   >
   > In the reference topology, `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

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

   - **Content Server Instance Folder:** `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs`

     Make sure this directory exists or is created before you save the configuration.

   - **Native File Repository Location:** `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs/vault`

     Make sure this directory exists or is created before you save the configuration.

   - **WebLayout Folder:** `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs/weblayout`

     Make sure this directory exists or is created before you save the configuration.

- **User Profile Folder:** `/u01/oracle/config/domains/WCCDomain/WCC_` `Cluster/cs/data/users/profiles`

  Make sure this directory exists or is created before you save the configuration.

- **Server Socket Port:** `4444`

- **Incoming Socket Connection Address Security Filter:** A pipe-delimited list of the local host and the server IP addresses:

  `127.0.0.1|WCCHOST1-IP|WCCHOST2-IP|WEBHOST1-IP|WEBHOST2-IP|WCCUIHOST1|WCCUIH` `OST2|ucminternal.example.com|`*load-balancer-host-name*

> **Note:** This will be changed later to a host name-based list (see Section 13.5.11, "Adding the Imaging Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content"). At this point, you need the connections to be allowed for operations that will be done before the security filter is changed to host names.

- **WebServer HTTP/HTTPS Address:** `wcc.example.com:443`

- **Web Address is HTTPS:** Select this checkbox.

- **Server Instance Name:** `WCC_Cluster`

- **Server Instance Label:** `WCC_Cluster`

- **Server Instance Description:** WebCenter Content cluster

- **Auto_Number Prefix:** `WCC_Cluster-`

3. Click **Submit** when finished, and restart the Managed Server, using the WebLogic Server Administration Console.

10.4.4 Updating the cwallet File in the Administration Server

Content Server updates the `cwallet.sso` file located in the *MSERVER_ HOME*`/config/fmwconfig` directory when it starts. This change needs to be propagated back to the Administration Server. To do this, copy the file to *ASERVER_ HOME*`/config/fmwconfig` on WCCHOST1 using the following command on WCCHOST1 (all on a single line):

```
cp -p MSERVER_HOME/config/fmwconfig/cwallet.sso ASERVER_HOME/config/fmwconfig
```

In the reference topology, *ASERVER_HOME* is the `/u01/oracle/config/domains/WCCDomain` directory.

> **Note:** If any operation is performed in a WLS_WCC*n* server that modifies the `cwallet.sso` file in the *MSERVER_ HOME*`/config/fmwconfig/` directory, the file will have to be immediately copied to the Administration Server domain configuration directory on WCCHOST1 at *ASERVER_ HOME*`/config/fmwconfig`.

10.4.5 Starting the WLS_WCC2 Managed Server and Configuring Content Server

After you start the WLS_WCC2 Managed Server, you can configure Content Server through the web interface.

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** tree on the left.

   b. Click **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. For possible causes, see Section 19.13, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology."

To configure Content Server:

1. Log in to WLS_WCC2 at `http://WCCHOST2:16200/cs` using your Oracle WebLogic Server 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 `ASERVER_HOME/WCC_Cluster`.
   >
   > In the reference topology, `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

2. Change the following values on the server configuration page:

   - **Content Server Instance Folder:** Set this to `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs`.

   - **Native File Repository Location:** Set this to `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs/vault`.

   - **WebLayout Folder:** Set this to `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs/weblayout`.

   - **User Profile Folder:** Set this to `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs/data/users/profiles`.

   - **Content Server URL Prefix:** `/cs/` (default value)

   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.

10.4.6 Validating GridLink Data Sources for WebCenter Content

After the servers are started, verify that the GridLink data sources are correctly configured and that the ONS setup is correct. Perform these procedures for every GridLink data source created.

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.

5. Click the **Testing** tab (Figure 10–9), select one of the servers, and click **Test Data Source**.

Figure 10–9   Testing a GridLink Data Source for WebCenter Content
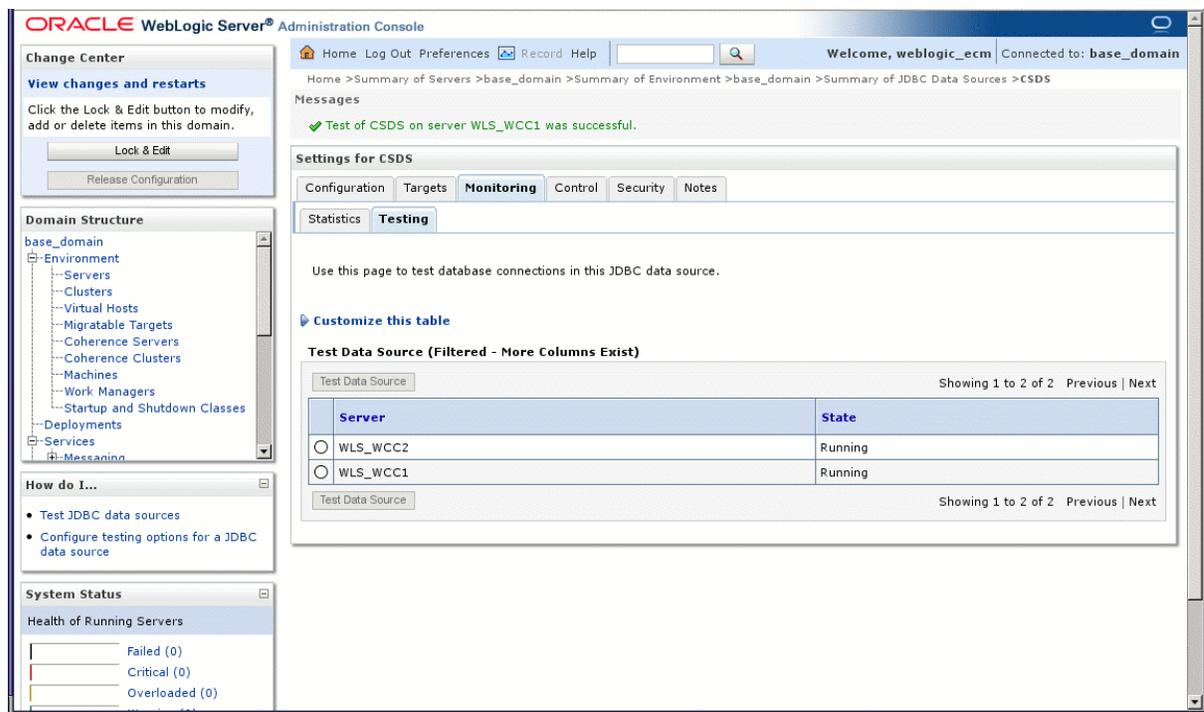
The test should be successful if the configuration is correct.

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. In the **Domain Structure** tree on the Administration Console, expand **Services**, then click **Data Sources**.

2. Click the name of a GridLink data source.

3. Click the **Monitoring** tab.

4. Click the name of the server (`WLS_WCC1`).

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

6. Select a server, and click **Test ONS**.

Figure 10–10   Testing the ONS Configuration for WebCenter Content

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@WCCDBHOST1 ~]$ srvctl status scan_listener
SCAN Listener LISTENER_SCAN1 is enabled
SCAN listener LISTENER_SCAN1 is running on node WCCDBHOST1
SCAN Listener LISTENER_SCAN2 is enabled
SCAN listener LISTENER_SCAN2 is running on node WCCDBHOST2
SCAN Listener LISTENER_SCAN3 is enabled
SCAN listener LISTENER_SCAN3 is running on node WCCDBHOST2


[orcl@WCCDBHOST1 ~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016


[orcl@WCCDBHOST1 ~]$ srvctl status nodeapps | grep ONS
ONS is enabled
ONS daemon is running on node: WCCDBHOST1
ONS daemon is running on node: WCCDBHOST2
```

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

10.4.7 Configuring Additional Parameters

Using a text editor, add the following options to each cluster node's *MSERVER_HOME*/ucm/cs/bin/intradoc.cfg file, where the directories specified are on a direct-bus-attached-controlled *local* disk and not a remote file system, such as a UNIX/Linux mounted NFS or clustered file system (like OCFS2, GFS2, or GPFS):

```
TraceDirectory=MSERVER_HOME/servers/WLS_WCCN/logs
EventDirectory=MSERVER_HOME/servers/WLS_WCCN/logs/event/
ArchiverDoLocks=true
DisableSharedCacheChecking=true
```

The trailing *N* should match your nodes' server names, like WLS_WCC1 is on WCCHOST1 and WLS_WCC2 is on WCCHOST2, and so on.

These changes will take effect after a restart of all WebCenter Content Managed Servers, at the end of the procedure described in Section 10.4.8, "Configuring Service Retries for Oracle WebCenter Content."

> **Note:** The directories can reside in any local disk path that you have determined to have enough space to hold the WebCenter Content logs and any trace that you may configure. The preceding paths are a suggestion.

10.4.8 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 configure service retries for Oracle WebCenter Content:

1. Go to Content Server at http://WCCHOST1:16200/cs, and log in using your WebLogic Server administration user name and password.

2. From the **Administration** tray or menu, choose **Admin Server**, then **General Configuration**.

3. On the General Configuration page, add the following parameter in the **Additional Configuration Variables** box:

   ```
   ServiceAllowRetry=true
   ```

4. Click **Save**, and restart all WebCenter Content Managed Servers, using the WebLogic Server Administration Console.

   > **Note:** The new parameter is included in the config.cfg file, which is at the following location:
   >
   > ```
   > /u01/oracle/config/domains/WCCDomain/WCC_
   > Cluster/cs/config/config.cfg
   > ```
   >
   > (You can also edit this file directly in a text editor. Remember to restart all WebCenter Content Managed Servers.)

10.5 Configuring Content Server for the WebCenter Content User Interface

If you are planning to use the WebCenter Content user interface (in addition to the native user interface for Content Server), you need to enable the following Content Server parameters:

- AutoSuggestConfig
- DynamicConverter
- FrameworkFolders

In addition, you need to set up the Remote Intradoc Client (RIDC) for communication between the WebCenter Content user interface and Content Server,

You can also set the following Content Server parameters for folders and searching, for the WebCenter Content user interface:

- `FoldersIndexParentFolderValues=true`
- `FldEnforceFolderFileNameUniqueness=true`
- `FldEnforceCaseInsensitiveNameUniqueness=true`
- `SearchIndexerEngineName=OracleTextSearch` or `SearchIndexerEngineName=DATABASE.METADATA`

For more information, see Section 15.2, "Preparing to Install and Configure the WebCenter Content User Interface."

10.6 Configuring Oracle HTTP Server with the WebCenter Content Cluster

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. Then you can validate access to the Managed Servers through the load balancer.

This section includes the following topics:

- Section 10.6.1, "Configuring Oracle HTTP Server for the WLS_WCC Managed Servers"
- Section 10.6.3, "Validating Access Through the Load Balancer"

10.6.1 Configuring Oracle HTTP Server for the WLS_WCC Managed Servers

To configure Oracle HTTP Server for the WLS_WCC Managed Servers:

1. For each of the web servers on WEBHOST1 and WEBHOST2, add the following lines to the *ORACLE_INSTANCE*/config/OHS/ohs1/moduleconf/wcc_vh.conf and *ORACLE_INSTANCE*/config/OHS/ohs2/moduleconf/wcc_vh.conf files:

```
# 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>
```

In the reference topology, *ORACLE_INSTANCE* is the `/u02/oracle/config/web1` or `/u02/oracle/config/web2` directory.

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

   `/u02/oracle/config/webN/bin/opmnctl restartproc ias-component=ohsX`

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

10.6.2 Enabling Access for Content Server Admin Applets

Because the SSL termination is configured on Oracle Web Tier for the enterprise deployment reference topology, the WebLogic Plug-In needs to be enabled for each WebCenter Content Managed Server for successful access to the Content Server Admin Applets.

To enable access for Content Server Admin Applets:

1. Log in to the WebLogic Server Administration Console at http://*host.domain:port*/console; for example:

   `http://ADMINVHN:7001/console`

2. On the **Environment** tab, click **Servers**.

3. Click **WLS_WCC1**.

4. Click the **General** tab on the **Configuration** tab, and go to the Advanced section.

5. Select the checkbox for **WebLogic Plug-In Enabled**.

6. Click the **Save** button to save the change.

7. Restart the WLS_WCC1 Managed Server from the Administration Console.

8. Perform steps 2-6 for the WLS_WCC2 Managed Server.

10.6.3 Validating Access Through the Load Balancer

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://wcc.example.com/cs` to verify that 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://wcc.example.com/cs` to verify that it is functioning properly.

You can verify the cluster node to which you were directed after the traffic balancing provided through your load balancer and then again through the web tier.

To verify the cluster node:

1. Log in to the following WebCenter Content page, using your Administration user and password credentials:

```
https://wcc.example.com/cs/idcplg?IdcService=CONFIG_INFO
```

2. Browse to the Administration/Configuration for *instance* page.

3. In the Options and Others section of the page, click **Java Properties** on the right.

4. Obtain the value for **weblogic.Name**.

This value denotes the cluster node you are accessing at the moment.

10.7 Configuring Node Manager for the WLS_WCC Managed Servers

Oracle recommends using host name verification for 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. For more details, see Chapter 16, "Setting Up Node Manager for an Enterprise Deployment." The procedures in that chapter must be performed for the Oracle WebCenter Content deployment.

The procedures in Section 16.3, "Enabling Host Name Verification Certificates for Node Manager," must be performed for the hosts and WebCenter Content Managed Servers in the following table.

Host Name (*HOST*)	Virtual IP Address (*VIP*)	Server Name (*WLS_SERVER*)
WCCHOST1	n/a	WLS_WCC1
WCCHOST2	n/a	WLS_WCC2

10.8 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. For information about database backup, see the *Oracle Database Backup and Recovery User's Guide*.

To back up the installation at this point:

1. Back up Oracle Web Tier on WEBHOST1:

    a. Shut down the instance using `opmnctl`.

    ```
    /u02/oracle/config/webN/bin/opmnctl stopall
    ```

    b. Back up the Middleware home for Oracle Web Tier with the following command (as root):

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

    c. Back up the Oracle instance for Oracle Web Tier with the following command:

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

    d. Start the instance with `opmnctl`:

    ```
    cd /u02/oracle/config/webN/bin
    opmnctl startall
    ```

2. Back up the database. This is a full database backup (either hot or cold) with 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 `/u01/oracle/config/domains/WCCDomain` directory. Run the following command on WCCHOST1 to create the backup:

    ```
    tar -cvpf edgdomainback.tar /u01/oracle/config/domains/WCCDomain
    ```

11

Extending the Domain to Include Inbound Refinery

This chapter describes how to extend a domain to include Oracle WebCenter Content: Inbound Refinery, using the Fusion Middleware Configuration Wizard.

This chapter includes the following sections:

- Section 11.1, "Overview of Extending the Domain to Include Inbound Refinery"
- Section 11.2, "Extending the Domain for Inbound Refinery"
- Section 11.3, "Restarting the Administration Server"
- Section 11.4, "Completing Postconfiguration and Verification Tasks for Inbound Refinery"
- Section 11.5, "Configuring the Inbound Refinery Managed Servers"
- Section 11.6, "Validating the Configuration of the Inbound Refinery Managed Servers"
- Section 11.7, "Configuring Node Manager for WLS_IBR Managed Servers"

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

11.1 Overview of Extending the Domain to Include Inbound Refinery

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, each installed and configured on a separate machine. In the reference Oracle WebCenter Content enterprise deployment topology, Inbound Refinery will be configured on the same machine as Content Server.

Even though multiple Managed Servers are created in the process of extending the domain with Inbound Refinery in this enterprise deployment topology, each Inbound Refinery instance is completely independent. Inbound Refinery does not run in a cluster.

Extend the domain to include Oracle WebCenter Content: Inbound Refinery. Table 11–1 lists the steps for configuring WebCenter Content and other tasks required for extending the domain with Inbound Refinery Managed Servers.

Table 11–1   Steps for Extending the Domain with Inbound Refinery

Step	Description	More Information
Extend the domain for Inbound Refinery	Extend the Oracle WebLogic Server domain you created in Chapter 8, "Creating a Domain for an Enterprise Deployment."	Section 11.2, "Extending the Domain for Inbound Refinery"
Propagate the domain configuration to the Inbound Refinery Managed Servers	Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the Managed Server domain directories.	Section 11.4.1, "Propagating the Domain Configuration to WLS_IBR1 and WLS_IBR2"
Restart the Administration Server for the domain	Stop and then start the Administration Server to make the changes from the previous step take effect.	Section 11.3, "Restarting the Administration Server"
Start the Inbound Refinery Managed Servers	Start the WLS_IBR1 and WLS_IBR2 Managed Servers.	Section 11.4.2, "Starting the Inbound Refinery Managed Servers"
Configure the Inbound Refinery instances	Complete the initial configuration of Inbound Refinery on WLS_IBR1 and WLS_IBR	Section 11.5, "Configuring the Inbound Refinery Managed Servers"
Verify the Inbound Refinery configuration	Verify that a file with an extension recognized as valid for conversion is correctly converted on Content Server.	Section 11.6, "Validating the Configuration of the Inbound Refinery Managed Servers"
Configure host name verification for communication between Node Manager and the Managed Servers in the domain	Use certificates for the different addresses communicating with the Administration Server and other servers.	Section 11.7, "Configuring Node Manager for WLS_IBR Managed Servers"

11.2 Extending the Domain for Inbound Refinery

To complete the enterprise deployment topology, you must extend the domain created in Chapter 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 for Inbound Refinery:

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. Shut down all Managed Servers in the domain.

3. On WCCHOST1, change the directory to the location of the 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
   ```

4. Start the Configuration Wizard:

   ```
   ./config.sh
   ```

5. On the Welcome screen, select **Extend an existing WebLogic domain**, and click **Next**.

6. On the Select a WebLogic Domain Directory screen, select the WebLogic Server domain directory (*ASERVER_HOME*), and click **Next**.

7. On the Select Extension Source screen, perform the following steps:

   ■ Select **Extend my domain automatically to support the following added products**.

   ■ Select the following products:

      – **Oracle Universal Content Management - Inbound Refinery**

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

      – **Oracle Enterprise Manager Plugin for IBR** (automatically selected when you select **Oracle Universal Content Management - Inbound Refinery**.)

Figure 11–1   Select Extension Source Screen for Inbound Refinery
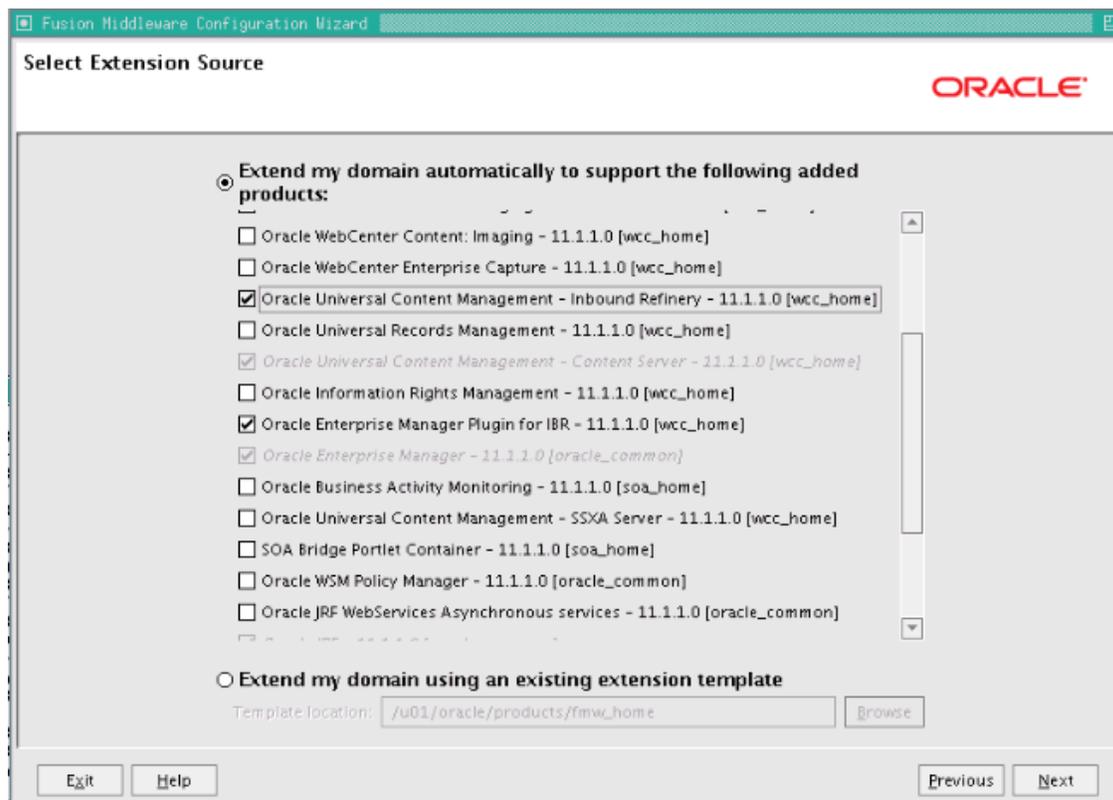
The following products are grayed out if they were selected when you created the domain (Section 8.3) or extended it for WebCenter Content (Section 10.2).

■ **Basic WebLogic Server Domain**

■ **Oracle Universal Content Management - Content Server**

■ **Oracle Enterprise Manager**

■ **Oracle JRF**

Click **Next**.

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

9. On the Test JDBC Component Schema screen, nothing needs to be done. Click **Next** to continue.

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

   ■ **Managed Servers, Clusters and Machines**

   ■ **Deployment and Services**

   Click **Next**.

11. On the Configure Managed Servers screen (Figure 11–2), add a Managed Server for Inbound Refinery and configure the Inbound Refinery servers.

Figure 11–2   Configure Inbound Refinery Managed Servers
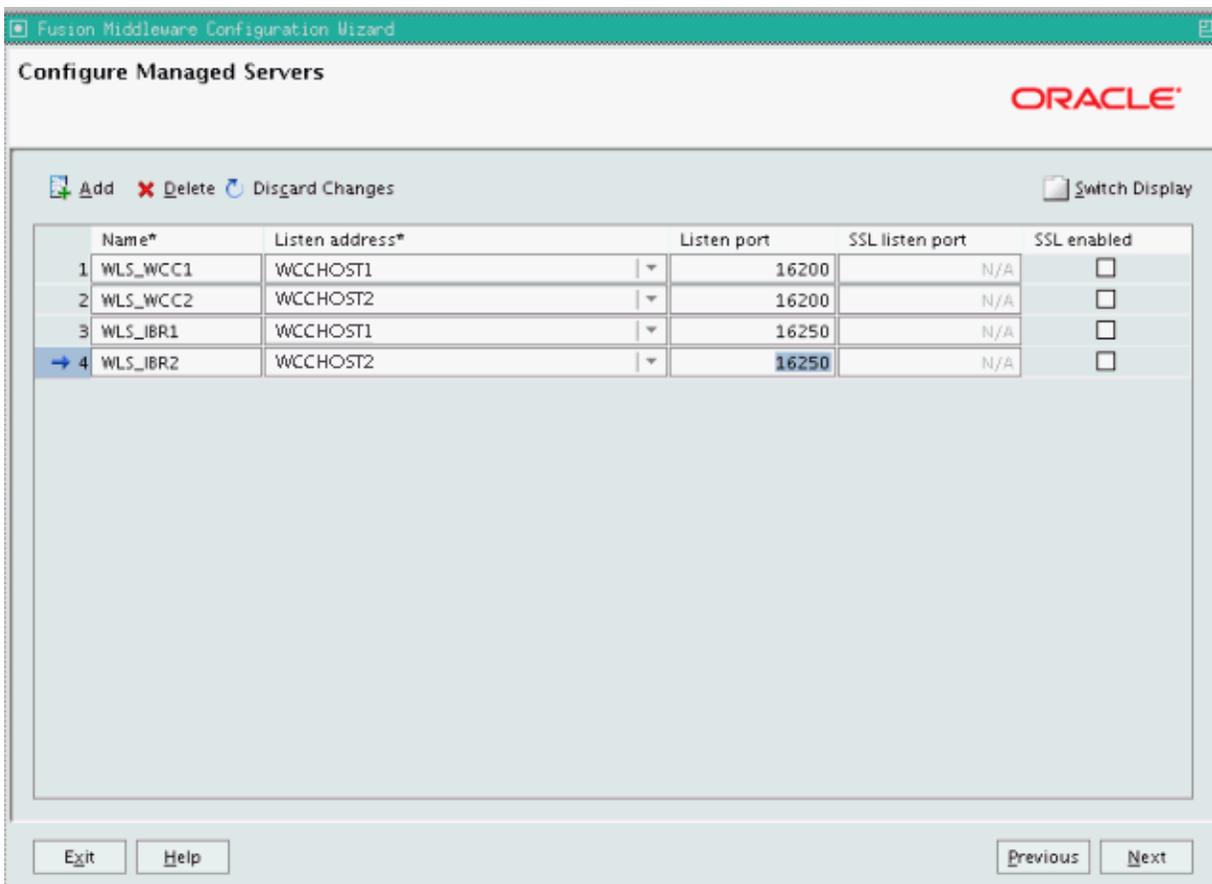
One server is created automatically. Rename this server to `WLS_IBR1`, and add a new server named `WLS_IBR2`. Give these servers the attributes listed in Table 11–2. Do not modify the other servers that are shown on this screen.

Table 11–2   Managed Servers for Inbound Refinery

Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
WLS_IBR1	WCCHOST1	16250	n/a	No
WLS_IBR2	WCCHOST2	16250	n/a	No

Click **Next**.

12. On the Configure Clusters screen, click **Add** and enter `IBR_Servers`, which Table 11–3 describes. Do not modify any other cluster that appears on this screen.

Table 11–3   Configuration for Managing Inbound Refinery Servers

Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
IBR_Servers	unicast	n/a	n/a	Leave empty.

Click **Next**.

> **Note:**   All Inbound Refinery instances are completely independent. The cluster is used for management purposes only. You can assign Inbound Refinery to a server group, but it does not run as a cluster because each Inbound Refinery Managed Server runs independently.

13. On the Assign Servers to Clusters screen (Figure 11–3), assign the following servers to **IBR_Servers**:

–   **WLS_IBR1**

–   **WLS_IBR2**

Do not modify any other assignments that appear on this screen.

Figure 11–3   Assign Inbound Refinery Servers to a Server Group
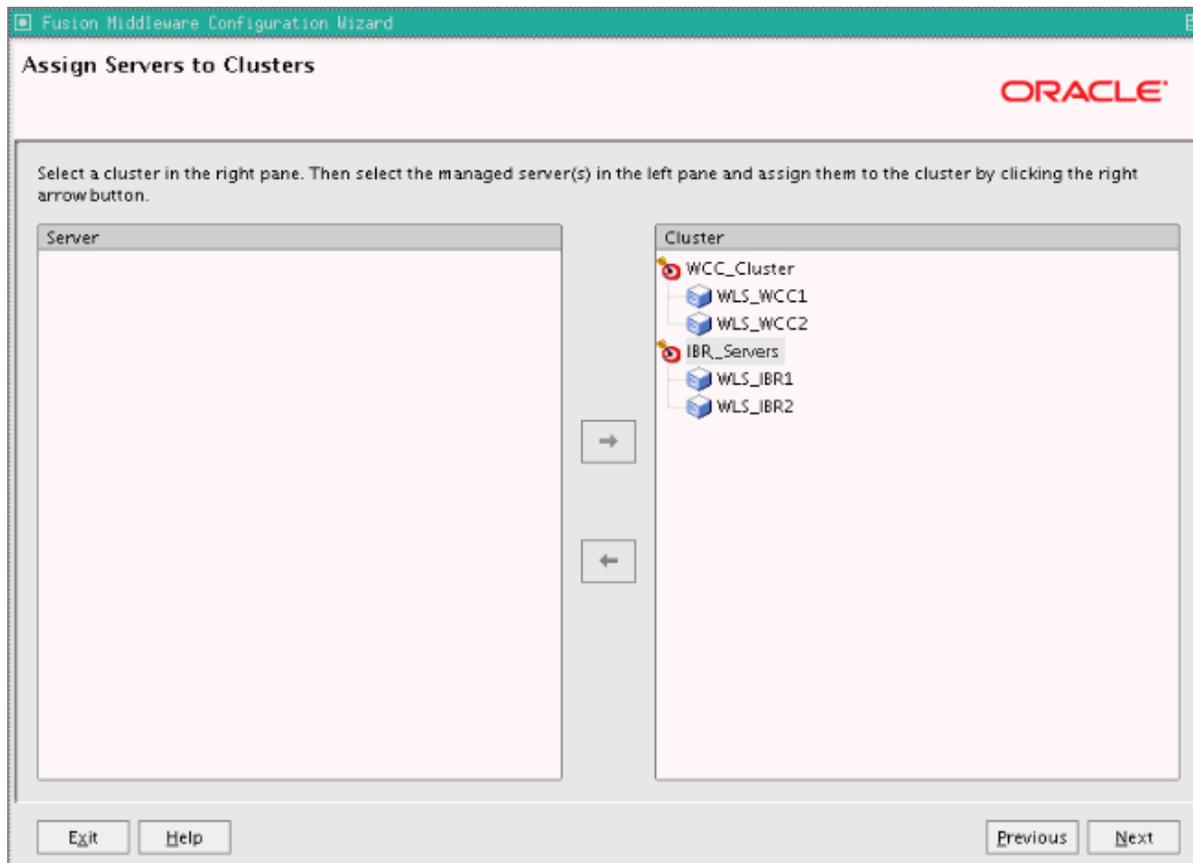
Click **Next**.

14. On the Configure Machines screen, click **Next**.

    You do not need to add any machines here. The machines configured earlier, as described in Section 10.2, "Extending the Domain for WebCenter Content," will be used for all Managed Servers configured on WCCHOST1 and WCCHOST2.

15. On the Assign Servers to Machines screen (Figure 11–4), assign the Inbound Refinery Managed Servers to machines as follows:

    ■ Assign **WLS_IBR1** to **WCCHOST1**.

    ■ Assign **WLS_IBR2** to **WCCHOST2**.

Figure 11–4   Assign Inbound Refinery Servers to Machines
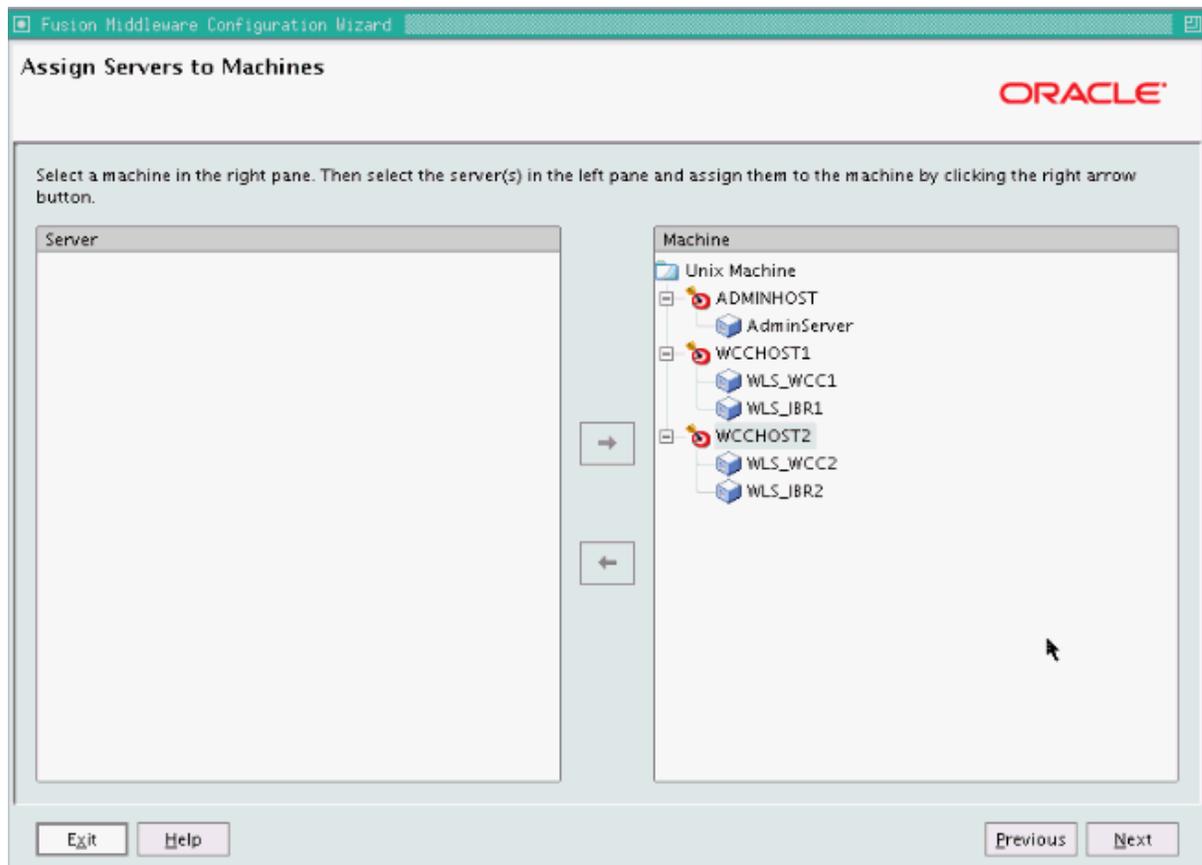
Click **Next**.

16. On the Target Deployments to Clusters or Servers screen, make sure that **EM Application** is targeted only to **AdminServer**.

    Click **Next**.

17. On the Target Services to Clusters or Servers screen, select all OPSS-related data sources to be deployed to **IBR_Servers**, as Figure 11–5 shows:

    ■ **opss-audit-viewDS**

    ■ **opss-audit-DBDS**

    ■ **opss-DBDS**

Figure 11–5 Target Services for Inbound Refinery
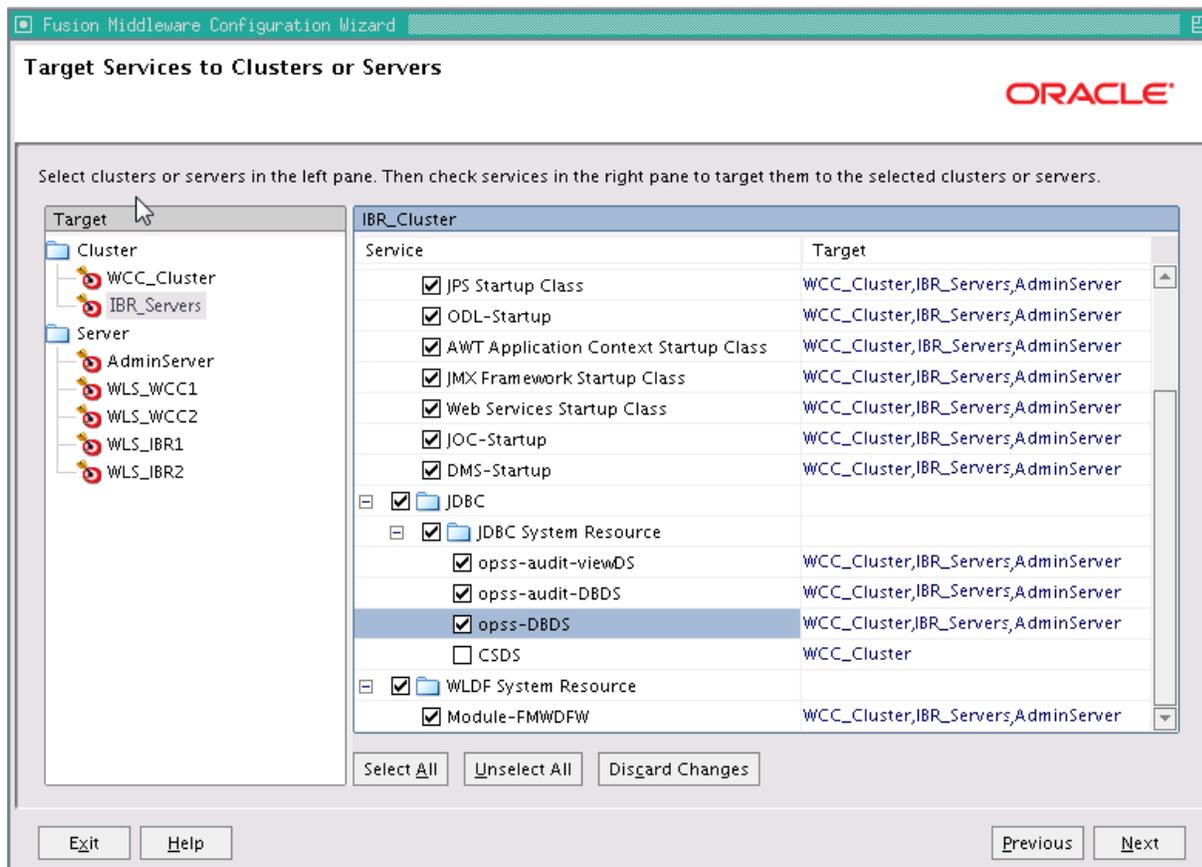
Click **Next**.

18. On the Configuration Summary screen, click **Extend**.

19. On the Creating Domain screen, click **Done**.

11.3 Restarting the Administration Server

You need to restart the Administration Server to make the domain extension changes take effect, using the Node Manager `nmKill` and `nmStart` commands through the Oracle WebLogic Scripting Tool (WLST), as described in Section 10.3, "Restarting the Administration Server." You can use the Administration Console instead of `nmKill` to stop the Administration Server. Log in to the Administration Console using the credentials for the `weblogic` user.

11.4 Completing Postconfiguration and Verification Tasks for Inbound Refinery

The following sections describe how to do postconfiguration and verification tasks for Inbound Refinery:

■ Section 11.4.1, "Propagating the Domain Configuration to WLS_IBR1 and WLS_IBR2"

■ Section 11.4.2, "Starting the Inbound Refinery Managed Servers"

11.4.1 Propagating the Domain Configuration to WLS_IBR1 and WLS_IBR2

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

To propagate the domain configuration to the Inbound Refinery Managed Servers:

1. Create a copy of the Managed Server domain directory and the Managed Server applications directory.

2. Run the following `pack` command on WCCHOST1 to create a template pack:

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

   ```
   ./pack.sh -managed=true -domain=ASERVER_HOME -template=edgdomaintemplateIBR.jar
   -template_name=edgdomain_templateIBR
   ```

   In the reference topology, `ORACLE_COMMON_HOME` is the `/u01/oracle/products/fmw_home/oracle_common` directory, and `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

3. Run the following `unpack` command on WCCHOST1 to propagate the template created in the preceding step to the WLS_IBR1 domain directory:

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

   ```
   ./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateIBR.jar -app_
   dir=APPLICATION_HOME -overwrite_domain=true
   ```

   In the reference topology, `MSERVER_HOME` is the `/u02/oracle/config/domains/WCCDomain` directory, and `APPLICATION_HOME` is the `/u01/oracle/config/applications/WCCDomain` directory.

   Notes:

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

   - The `APPLICATION_HOME` directory gets backed up with this `unpack` command.

   - 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.

   ---

4. Run the following command on WCCHOST1 to copy the template pack created in step 1 to WCCHOST2:

   ```
   scp edgdomaintemplateIBR.jar oracle@WCCHOST2:ORACLE_COMMON_HOME/common/bin
   ```

5. Run the `unpack` command on WCCHOST2 to unpack the propagated template to the WLS_IBR1 domain directory.

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

   ```
   ./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateIBR.jar -app_
   dir=APPLICATION_HOME -overwrite_domain=true
   ```

> **Notes:**
>
> - Make sure to run `unpack` from the *ORACLE_COMMON_HOME*/common/bin directory, not from *WL_HOME*/common/bin.
>
> - The *APPLICATION_HOME* directory gets backed up with this `unpack` command.

6. Restart the Administration Server to make these changes take effect, stopping it with the `nmKill` command, or with the Administration Console, and then starting it with the `nmStart` command, as described in Section 10.3, "Restarting the Administration Server." Log in to the Administration Console using the credentials for the `weblogic` user.

11.4.2 Starting the Inbound Refinery Managed Servers

After you propagate the domain configuration, start the Inbound Refinery Managed Servers.

To start the WLS_IBR1 Managed Server on WCCHOST1:

1. Log in to the Oracle WebLogic Server Administration Console at `http://admin.example.com:7001/console`.

2. Start the WLS_IBR1 Managed Server through the Administration Console, as follows:

   a. Expand the **Environment** node in the **Domain Structure** tree on the left.

   b. Click **Servers**.

   c. On the Summary of Servers page, click the **Control** tab.

   d. Select **WLS_IBR1** from the **Servers** column of the table.

   e. Click **Start**.

3. 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. For possible causes, see Section 19.13, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology."

4. Repeat the preceding steps to start the WLS_IBR2 Managed Server on WCCHOST2.

11.5 Configuring the Inbound Refinery Managed Servers

To initialize the configuration of an Inbound Refinery Managed Server, you need to access it only once through HTTP. You can do this directly, at the Managed Server's listen address. An Inbound Refinery instance should not be placed behind an HTTP server.

All subsequent access to the Inbound Refinery instance 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 Content Server instance with all Inbound Refinery instances. The process for configuring Content Server is to add each Inbound Refinery instance as a provider. You also need to perform some postinstallation steps with Inbound Refinery.

The following sections describe the procedures for postinstallation configuration of each Inbound Refinery instance:

- Section 11.5.1, "Configuring Inbound Refinery Settings"
- Section 11.5.2, "Specifying the Font Path"
- Section 11.5.3, "Configuring Document Conversion"
- Section 11.5.4, "Setting Up Content Server to Send Jobs to Inbound Refinery for Conversion"

11.5.1 Configuring Inbound Refinery Settings

After you start the Inbound Refinery Managed Servers, configure the settings for each server on its postinstallation configuration screen.

To configure the settings for each Inbound Refinery instance:

1. Access the Inbound Refinery postinstallation configuration screen at the following URL, in which *N* is 1 or 2:

   `http://WCCHOSTN:16250/ibr/`

2. On the Configuration screen, you will see Inbound Refinery Instance Identifier: *name*. Set the configuration settings for this instance as follows:

   - **Inbound Refinery Instance Folder:**
     /u01/oracle/config/domains/WCCDomain*/IBR_Servers/ibrN/*

     The directory path should be on a shared disk, and the directories should be created before the configuration is saved.

   - **Native File Repository Location:**
     /u01/oracle/config/domains/WCCDomain*/IBR_Servers/ibrN*/vault/

   - **WebLayout Folder:** /u01/oracle/config/domains/WCCDomain*/IBR_Servers/ibrN*/weblayout/

   - **User Profile Folders:** /u01/oracle/config/domains/WCCDomain*/IBR_Servers/ibrN*/data/users/profiles/

   - **Incoming Socket Connection Address Security Filter:** A pipe-delimited list of localhost and the server IP addresses:

     `127.0.0.1|WCCHOST1-IP|WCCHOST2-IP`

     This setting enables access from Content Server. The values for `WCCHOST1-IP` and `WCCHOST2-IP` should be the IP addresses of the machines with the 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.)

     The **Incoming Socket Connection Address Security Filter:** field accepts wildcards in the value; for example, 192.0.2.*.

You can change this value later by setting `SocketHostAddressSecurityFilter` in the `/u02/oracle/config/domains/WCCDomain/ucm/ibr/config/config.cfg` file and then restarting the Inbound Refinery Managed Server.

- **Server Socket Port:** Enter an unused port number, such as `5555`. This value is the number of the port for calling top-level services.

  Take note of the port number because you need it later for configuring Oracle WebCenter Content.

  Changing this field value changes the `IntradocServerPort` entry in `/u02/oracle/config/domains/WCCDomain/ucm/ibr/config/config.cfg`.

- **Server Instance Name:** Specify a name for the Inbound Refinery server instance.

  You can accept the default value or change it to a name that is more useful to you. Take note of the server name because you will need it later for 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, using the WebLogic Server Administration Console.

4. Repeat the preceding steps for each Inbound Refinery instance, using different names for the content folders.

11.5.2 Specifying the Font Path

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 that 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 *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

11.5.3 Configuring Document Conversion

Enable the components you need for document conversion on each Inbound Refinery Managed Server through the Component Manager.

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`

    `http://WCCHOSTN: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. From the **Administration** tray or menu, choose **Admin Server**, then **Component Manager**.

    b. On the Component Manager page, select **PDFExportConverter** under **Inbound Refinery** and any other components you want.

    `PDFExportConverter` uses Oracle Outside In Technology 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, using the WebLogic Server Administration Console.

    f. Set the primary web-viewable conversion to `PDF Export`:

    *   Select **Conversion Settings**, then select **Primary Web Rendition**.

    *   On the Primary Web-Viewable Rendition page, select **Convert to PDF using PDF Export**.

    *   Click **Update** to save your changes.

    After a restart, Inbound Refinery will use Outside In Technology PDF Export to convert files directly to PDF without the use of third-party applications.

    g. Restart the Inbound Refinery Managed Server, using the WebLogic Server Administration Console.

    > **Note:** For information about the conversion components, see "Configuring the Content Server Refinery Conversion Options" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

3. Restart the Administration Server and all Inbound Refinery Managed Servers.

    To restart the Administration Server, stop it first using the Administration Console, and then start it again as described in Section 8.4.3, "Starting the Administration Server on WCCHOST1." To restart the Managed Servers, use the WebLogic Server Administration Console.

11.5.4 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 the setup tasks described in the following sections for each Inbound Refinery Managed Server:

- Section 11.5.4.1, "Creating an Outgoing Provider"

- Section 11.5.4.2, "Enabling Components for Inbound Refinery on Content Server"

- Section 11.5.4.3, "Selecting File Formats To Be Converted"

11.5.4.1 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.

To create an outgoing provider for each Inbound Refinery instance:

1. Log in to Content Server at the following URL:

   ```
   http://WCCHOST1:16200/cs/
   ```

2. Open the **Administration** tray or menu, then choose **Providers**.

3. In the **Create a New Provider** table 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`.

   - **Server Port:** The value of the Server Socket Port field for the Inbound Refinery instance as specified in Section 11.5.1, "Configuring Inbound Refinery Settings"; for example, `5555`. This is the `IntradocServerPort` value in the Content Server `config.cfg` file.

   - **Instance Name:** The server instance name for Inbound Refinery as specified in Section 11.5.1, "Configuring Inbound Refinery Settings." This is the `IDC_Name` value in the Inbound Refinery `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 the Inbound Refinery Managed Server and Oracle WebCenter Content Server (WebCenter Content Managed Server), using the WebLogic Server Administration Console.

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 Fusion Middleware Managing Oracle WebCenter Content*.

11.5.4.2 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 Content Server at the following URL:

   ```
   http://WCCHOST1:16200/cs/
   ```

2. From the **Administration** tray or menu, choose **Admin Server**, then **Component Manager**.

3. On the Component Manager page, select **Inbound Refinery**, then select components that you want to enable under Inbound Refinery, such as **XMLConverterSupport**, and then click **Update**.

4. Restart Content Server by restarting the WebCenter Content Managed Server, using the WebLogic Server Administration Console.

11.5.4.3 Selecting File Formats To Be Converted

To tell 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 Content Server at the following URL:

   ```
   http://WCCHOST1:16200/cs/
   ```

2. Open the **Administration** tray or menu, then choose **Refinery Administration**, and then **File Formats Wizard** to open the File Formats Wizard page

   This page 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 "Managing File Types" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

11.6 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 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.

For information about the check-in and check-out procedures, see "Uploading Documents" and "Checking Out and Downloading Files" in *Oracle Fusion Middleware Using Oracle WebCenter Content*.

For information about the conversion process, see "Configuring Content Servers to Send Jobs to Refineries" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

11.7 Configuring Node Manager for WLS_IBR Managed Servers

Oracle recommends using host name verification for 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. For more details, see Chapter 16, "Setting Up Node Manager for an Enterprise Deployment." The procedures in that chapter must be performed for the Oracle WebCenter Content deployment.

The procedures in Section 16.3, "Enabling Host Name Verification Certificates for Node Manager," must be performed for the hosts and Inbound Refinery Managed Servers in the following table.

Host Name (*HOST*)	Virtual IP Address (*VIP*)	Server Name (*WLS_SERVER*)
WCCHOST1	n/a	WLS_IBR1
WCCHOST2	n/a	WLS_IBR2

12

Extending the Domain to Include Oracle SOA Suite Components

This chapter describes how to extend the domain created in Chapter 8, "Creating a Domain for an Enterprise Deployment," to include Oracle SOA Suite components and the Oracle WSM Policy Manager Server, using the Fusion Middleware Configuration Wizard.

This chapter contains the following sections:

- Section 12.1, "Overview of Extending the Domain to Include Oracle SOA Suite Components"

- Section 12.2, "Enabling VIP2 on WCCHOST1 and VIP3 on WCCHOST2"

- Section 12.3, "Extending the Domain for Oracle SOA Suite Components"

- Section 12.4, "Restarting the Administration Server"

- Section 12.5, "Configuring Oracle Coherence for Deploying Composites"

- Section 12.6, "Completing Postconfiguration and Verification Tasks for Oracle SOA Suite"

- Section 12.7, "Configuring the Java Object Cache for Oracle Web Services Manager"

- Section 12.8, "Configuring Oracle HTTP Server with the Extended Domain"

- Section 12.9, "Configuring a Default Persistence Store for Transaction Recovery"

- Section 12.10, "Configuring Node Manager for the WLS_SOA Managed Servers"

- Section 12.12, "Backing Up the Installation"

Notes:

- Oracle SOA Suite is required only if your enterprise deployment topology includes Oracle WebCenter Content: Imaging.

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

12.1 Overview of Extending the Domain to Include Oracle SOA Suite Components

The instructions in this chapter are based on an assumption that a SOA Oracle home (binaries) has already been installed and is available from WCCHOST1 and WCCHOST2 and that a domain with an Administration Server has been created. This is the domain that will be extended to support Oracle SOA Suite components.

Extend the Oracle WebLogic Server domain to include Oracle SOA Suite components. Table 12–1 lists the steps for configuring Oracle SOA Suite and other tasks required for extending the domain for Oracle SOA Suite components.

Table 12–1   Steps for Extending the Domain for Oracle SOA Suite Components

Step	Description	More Information
Prepare for extending the domain for Oracle SOA Suite components	Enable a virtual IP address mapping for each of the host names for the Oracle SOA Suite WebLogic Server cluster.	Section 12.2, "Enabling VIP2 on WCCHOST1 and VIP3 on WCCHOST2"
Extend the domain for Oracle SOA Suite components	Extend the WebLogic Server domain you created in Chapter 8, "Creating a Domain for an Enterprise Deployment."	Section 12.3, "Extending the Domain for Oracle SOA Suite Components"
Configure Oracle Coherence for deploying composites	Configure Oracle Coherence to use unicast communication for deploying composites.	Section 12.5, "Configuring Oracle Coherence for Deploying Composites"
Complete postconfiguration and verification tasks	Follow these instructions for disabling host name verification, restarting Node Manager, propagating the domain configuration, starting and validating the Managed Servers, and validating GridLink data sources.	Section 12.6, "Completing Postconfiguration and Verification Tasks for Oracle SOA Suite"
Configure the Java Object Cache (JOC) among all the servers running Oracle Web Services Manager (Oracle WSM)	Configure a local cache to increase the performance of Oracle WSM.	Section 12.7, "Configuring the Java Object Cache for Oracle Web Services Manager"
Configure Oracle HTTP Server with the extended domain	Configure the Oracle HTTP Server with the Managed Servers, validate access, set the front-end HTTP host and port, and set the WebLogic Server cluster address for SOA_Cluster.	Section 12.8, "Configuring Oracle HTTP Server with the Extended Domain"
Configure a default persistence store	Configure a default persistence store for transaction recovery.	Section 12.9, "Configuring a Default Persistence Store for Transaction Recovery"
Configure host name verification for communication between Node Manager and the Managed Servers in the domain	Use certificates for the different addresses communicating with the Administration Server and other servers.	Section 12.10, "Configuring Node Manager for the WLS_SOA Managed Servers"
Configure server migration for the Oracle SOA Suite Managed Servers	Specify the Oracle SOA Suite Managed Server names, host names, and cluster name for migration.	vSection 12.11, "Configuring Server Migration for the WLS_SOA Managed Servers"
Back up the Oracle SOA Suite configuration	Back up the newly extended domain configuration.	Section 12.12, "Backing Up the Installation"

12.2 Enabling VIP2 on WCCHOST1 and VIP3 on WCCHOST2

The Oracle WebCenter Content domain uses virtual host names as the listen addresses for the Oracle SOA Suite Managed Servers. If you have not previously done so, you must enable a virtual IP address mapping from VIP2 to WCCHOST1VHN1 on WCCHOST1 and from VIP3 to WCCHOST2VHN1 on WCCHOST2, and you must correctly resolve the virtual host names in the network system used by the topology, with either DNS Server or `/etc/hosts` resolution.

To enable the virtual IP addresses, follow the procedure described in Section 6.6, "Enabling Virtual IP Addresses" if you have not yet completed it. These virtual IP addresses and virtual host names are required to enable server migration for the Oracle SOA Suite servers. You can configure server migration for the Oracle SOA Suite servers later for high availability purposes. For more information about configuring server migration, see Chapter 17, "Configuring Server Migration for an Enterprise Deployment."

12.3 Extending the Domain for Oracle SOA Suite Components

Use the 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.

> **Notes:** ■ Oracle SOA Suite is only required if the enterprise deployment topology requires Oracle WebCenter Content: Imaging.
>
> ■ 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 *Administrator's Guide*.

To extend the domain for Oracle SOA Suite components:

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. Shut down all Managed Servers in the domain.

3. On WCCHOST1, 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
   ```

4. Start the Configuration Wizard:

   ```
   ./config.sh
   ```

5. On the Welcome screen, select **Extend an Existing WebLogic Domain**, and click **Next**.

6. On the Select a WebLogic Domain Directory screen, select the WebLogic Server domain directory (*ASERVER_HOME*), and click **Next**.

7. On the Select Extension Source screen, which Figure 12–1 shows, perform the following steps:

    a. Select **Extend my domain automatically to support the following added products**.

    b. Select these products:

       * **Oracle SOA Suite**

       * **Oracle WSM Policy Manager**

       The following products are grayed out if they were selected when you created the domain (Section 8.3) or extended it for WebCenter Content (Section 10.2) or Inbound Refinery (Section 11.2).

       * **Basic WebLogic Server Domain**

       * **Oracle Universal Content Management - Inbound Refinery**

       * **Oracle Universal Content Management - Content Server**

       * **Oracle Enterprise Manager Plugin for IBR**

       * **Oracle Enterprise Manager**

       * **Oracle JRF**

Figure 12–1   Select Extension Source Screen for Oracle SOA Suite
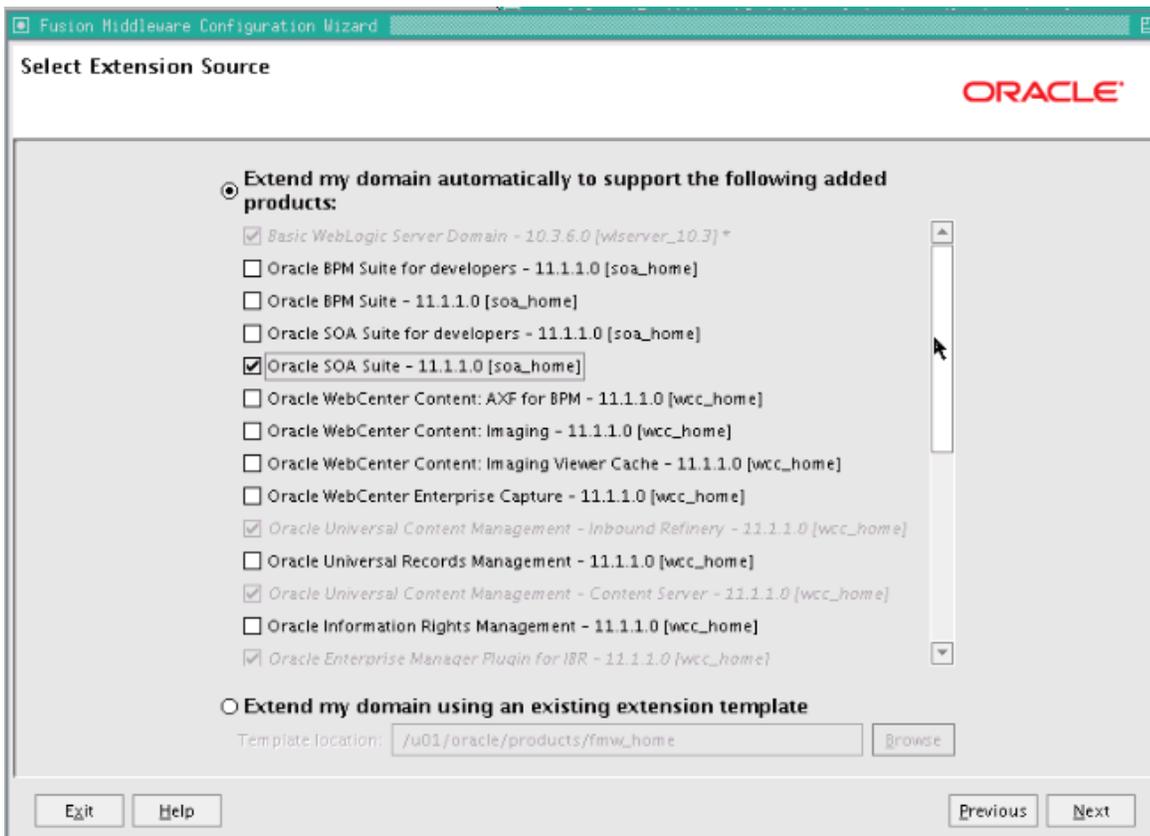
    c. Click **Next**.

8. If you get a `Conflict Detected` message that Oracle JRF is already defined in the domain, select the **Keep Existing Component** option and click **OK**.

9. On the Configure JDBC Component Schema screen, which Figure 12–2 shows, perform the following steps:

    a. Select the rows **SOA Infrastructure**, **User Messaging Service**, **OWSM MDS Schema**, and **SOA MDS Schema**.

    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 12–2   Configure JDBC Component Schema Screen for Oracle SOA Suite
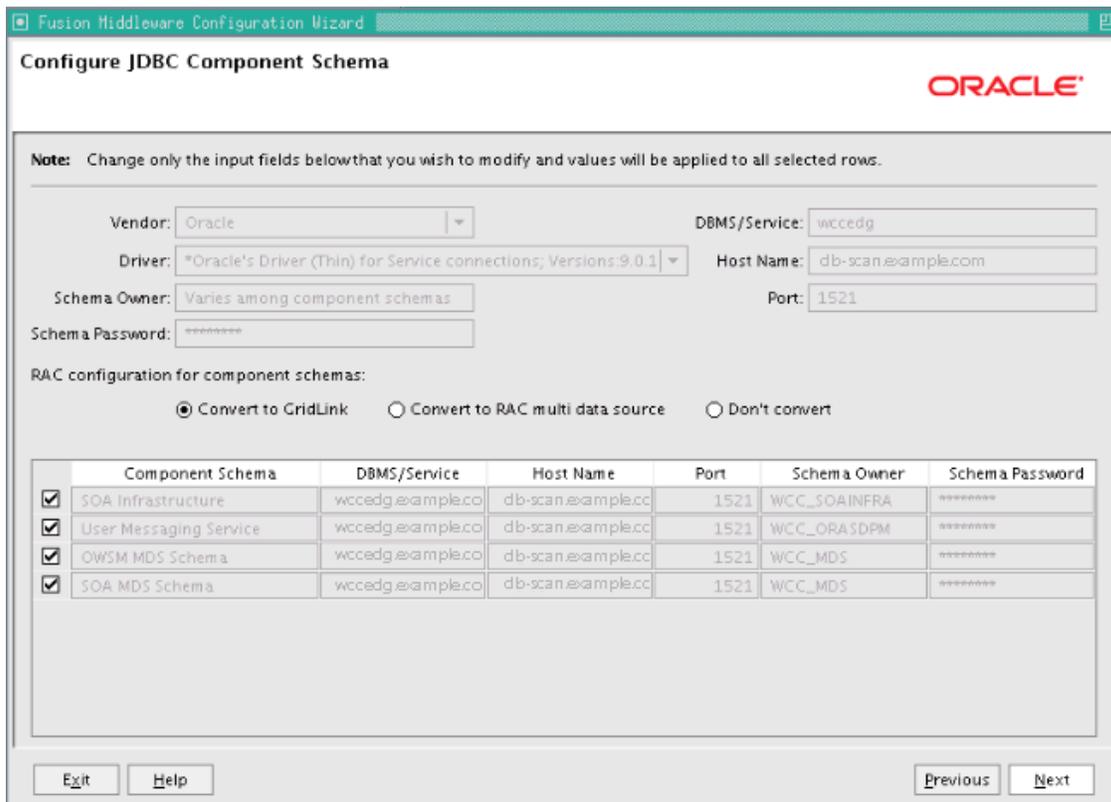
    c. Click **Next**.

10. On the Configure GridLink RAC Component Schema screen, which Figure 12–3 shows, perform the following steps:

    a. Select only the **SOA Infrastructure** row.

Figure 12–3   Configure GridLink RAC Component Schema Screen for Oracle SOA Suite

b. Enter values for the following fields, specifying the connection information for the GridLink RAC database that was seeded through RCU:

–   **Driver:** Select **Oracle's Driver (Thin) for GridLinkConnections; Versions: 11 and later**.

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

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

This book uses `WCC` 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>show parameter remote_listener;

NAME              TYPE        VALUE
-----             ------      -------
remote_listener   string      db-scan.example.com:1521
```

> **Note:** For Oracle Database 11*g*, use the virtual IP address and port of each database instance listener, as in these examples:
>
> ```
> wccdbhost1-vip.example.com (port 1521)
> ```
>
> ```
> wccdbhost2-vip.example.com (1521)
> ```

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

```
[orcl@WCCDBHOST2 ~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016
```

> **Note:** For Oracle Database 11*g*, use the host name and port of each database's ONS service, as in these examples:
>
> ```
> wccdbhost1.example.com (port 6200)
> ```
>
> ```
> wccdbhost2.example.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**.

> **Note:** Oracle recommends using the database used for Oracle Identity Management (see Chapter 18, "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 on 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. On the Test JDBC Component Schema screen, (Figure 12–4), 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 12–4   Test JDBC Component Schema Screen for Oracle SOA Suite
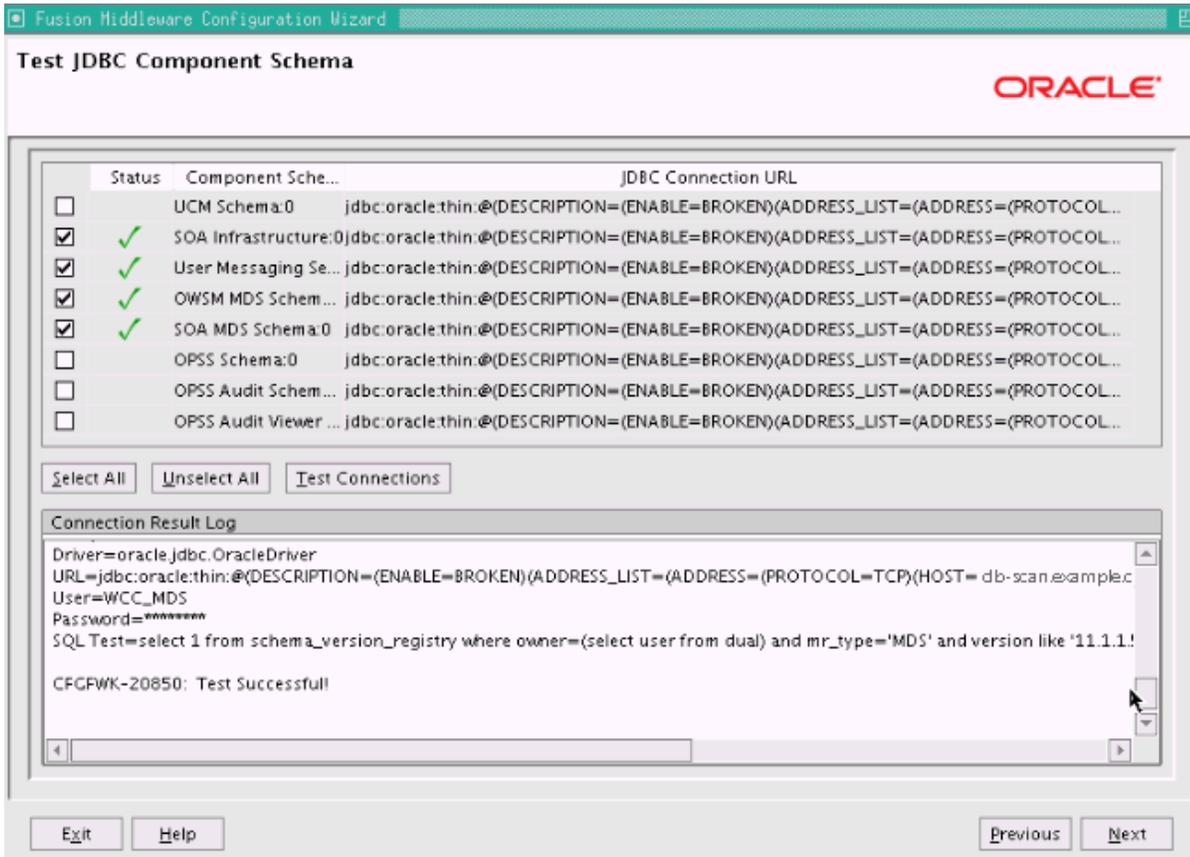
Click **Next** when all the connections are successful.

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

- **JMS Distributed Destination**

- **Managed Servers, Clusters and Machines**

- **Deployments and Services**

- **JMS File Store**

Click **Next**.

13. On the Select JMS Distributed Destination Type screen, perform the following steps:

- Select **UDD** from the drop-down list for **UMSJMSystemResource**.

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

- Select **UDD** from the drop-down list for **BPMJMSModule**.

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

14. On 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 12–2. Do not modify any other servers that are shown on this screen.

Table 12–2   Managed Servers for Oracle SOA Suite

Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
WLS_SOA1	WCCHOST1VHN1	8001	n/a	No
WLS_SOA2	WCCHOST2VHN1	8001	n/a	No

Click **Next**.

15. On the Configure Clusters screen, add `SOA_Cluster`, which Table 12–3 describes.

Table 12–3   Cluster Configuration for Oracle SOA Suite

Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
SOA_Cluster	unicast	n/a	n/a	WCCHOST1VHN1:8001,WCCHOST2VHN1:8001

Click **Next**.

> **Note:**   For asynch 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 callbacks.
>
> 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. On the Assign Servers to Clusters screen, assign the following servers to **SOA_ Cluster**:

  – `WLS_SOA1`

  – `WLS_SOA2`

Do not modify any other assignments that appear on this screen.

Click **Next**.

17. On the Configure Machines screen, delete **LocalMachine**, which appears by default, open the **Unix Machine** tab, and click **Next**.

You do not need to add any machines here. The machines configured earlier, as described in Section 10.2, "Extending the Domain for WebCenter Content," will be used for all Managed Servers configured on WCCHOST1 and WCCHOST2.

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

- **ADMINHOST:**

  – AdminServer

- **WCCHOST1:**

  – WLS_SOA1

- **WCCHOST2:**

  – WLS_SOA2

Click **Next**.

19. On the Target Deployments to Clusters or Servers screen, make sure that targeting is done as follows:

- The **usermessagingserver** and **usermessagingdriver-email** deployments are targeted only to **SOA_Cluster**. (The **usermessaging-xmpp**, **usermessaging-smpp**, and **usermessaging-voicexml** applications are optional.)

- **WSM-PM** is targeted only to **SOA_Cluster**.

- The **oracle.rules#***, **oracle.sdp.***, and **oracle.soa.*** libraries are targeted only to **SOA_Cluster**.

- **EM Application** is targeted only to **AdminServer**.

Click **Next**.

20. On the Target Services to Clusters or Servers screen, select all OPSS-related data sources to be deployed to **SOA_Cluster**, as Figure 12–5 shows:

- **opss-audit-viewDS**

- **opss-audit-DBDS**

- **opss-DBDS**

Figure 12–5   Target Services to the SOA Cluster
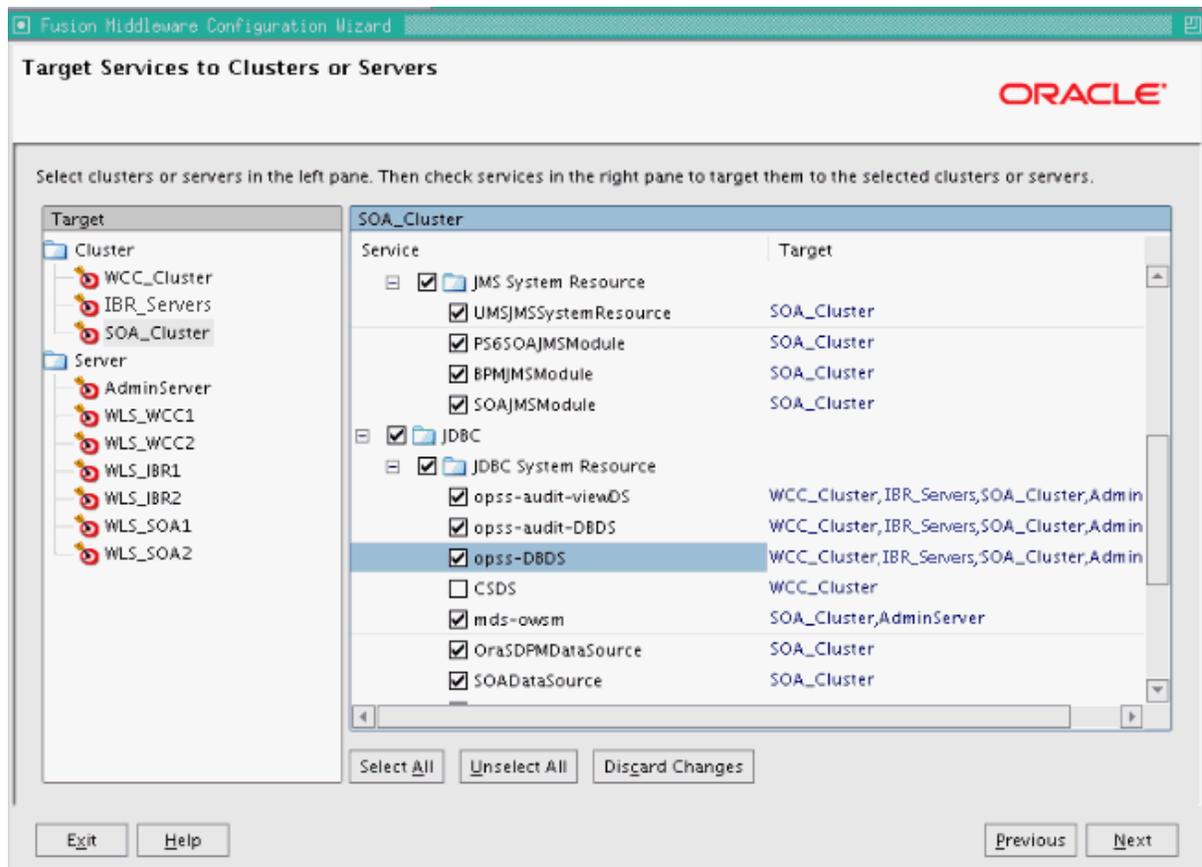
Click **Next**.

21. On the Configure JMS File Stores screen (Figure 12–6), enter the shared directory location specified for your JMS stores, as recommended in Section 4.4, "Recommended Locations for Different Directories." For example:

    `ASERVER_HOME/SOA_Cluster/jms`

    This directory should be created before you extend the domain.

    In the reference topology, `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

Figure 12–6 JMS File Stores for the SOA Cluster
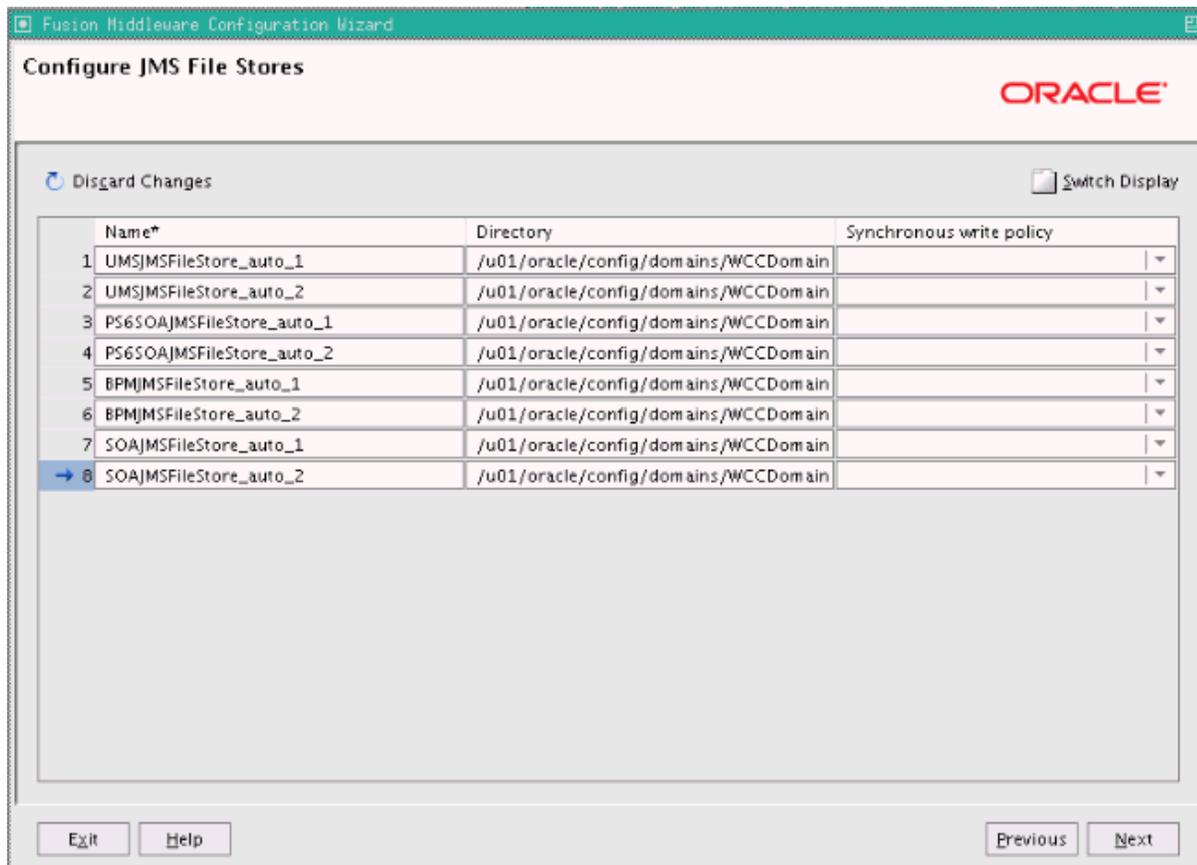
Click **Next**.

22. On the Configuration Summary screen, click **Extend**.

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

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

12.4 Restarting the Administration Server

You need to restart the Administration Server to make the domain extension changes take effect, using the Node Manager `nmKill` and `nmStart` commands through the Oracle WebLogic Scripting Tool (WLST), as described in Section 10.3, "Restarting the Administration Server." You can use the Administration Console instead of `nmKill` to stop the Administration Server. Log in to the Administration Console using the credentials for the `weblogic` user.

12.5 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 IP addresses 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.

12.5.1 Enabling Communication for Deployment Using Unicast Communication

Specify the nodes using the `tangosol.coherence.wkan` system property, where *n* is a number in the range `1` to `9`. You can specify up to 9 nodes as Well Known Addresses, but the cluster can have more than 9 nodes. Start the numbering at 1. This numbering must be sequential and must not contain gaps.

> **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.

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 (WCCHOST1VHN1 and WCCHOST2VHN1). Set this property by adding the `-Dtangosol.coherence.localhost` parameter to the **Arguments** field on the **Server Start** tab of the Oracle WebLogic Server Administration Console, shown in Figure 12–7.

> **Note:** WCCHOST1VHN1 is the virtual host name that maps to the virtual IP address where WLS_SOA1 is listening (in WCCHOST1). WCCHOST2VHN1 is the virtual host name that maps to the virtual IP address where WLS_SOA2 is listening (in WCCHOST2).

12.5.2 Specifying the Host Name Used by Oracle Coherence

Use the Administration Console to add a host name for Oracle Coherence to use.

To specify the host name used by Oracle Coherence:

1. Log in to the WebLogic Server Administration Console.

2. In the **Domain Structure** tree on the left, 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. On the **Configuration** tab, click the **Server Start** tab (illustrated in Figure 12–7).

7. Enter the following parameters for WLS_SOA1 and WLS_SOA2 in the **Arguments** field.

> **Note:** There should be no breaks in lines between the different -D parameters. Do not copy or paste the text to the **Arguments** text field in your Administration Console because this could result in HTML tags being inserted into the Java arguments. The text should not contain other text characters than those included the example that follows.

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

```
-Dtangosol.coherence.wka1=WCCHOST1VHN1
-Dtangosol.coherence.wka2=WCCHOST2VHN1
-Dtangosol.coherence.localhost=WCCHOST1VHN1
```

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

```
-Dtangosol.coherence.wka1=WCCHOST1VHN1
-Dtangosol.coherence.wka2=WCCHOST2VHN1
-Dtangosol.coherence.localhost=WCCHOST2VHN1
```

> **Note:** The Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying a different port (for example, 8089) using the `-Dtangosol.coherence.wkan.port` and `-Dtangosol.coherence.localport` startup parameters; for example:
>
> - WLS_SOA1 (enter the following text into the **Arguments** field on a single line, without a carriage return):
>
>   ```
>   -Dtangosol.coherence.wka1=WCCHOST1VHN1
>   -Dtangosol.coherence.wka2=WCCHOST2VHN1
>   -Dtangosol.coherence.localhost=WCCHOST1VHN1
>   -Dtangosol.coherence.localport=8089
>   -Dtangosol.coherence.wka1.port=8089
>   -Dtangosol.coherence.wka2.port=8089
>   ```
>
> - WLS_SOA2 (enter the following text into the **Arguments** field on a single line, without a carriage return):
>
>   ```
>   -Dtangosol.coherence.wka1=WCCHOST1VHN1
>   -Dtangosol.coherence.wka2=WCCHOST2VHN1
>   -Dtangosol.coherence.localhost=WCCHOST2VHN1
>   -Dtangosol.coherence.localport=8089
>   -Dtangosol.coherence.wka1.port=8089
>   -Dtangosol.coherence.wka2.port=8089
>   ```
>
> For more information about Coherence clusters, see the *Oracle Coherence Developer's Guide*.

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

> **Notes:**
>
> - 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.
> - 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.

Figure 12–7   Setting the Host Name on the Start Server Tab of the Administration Console
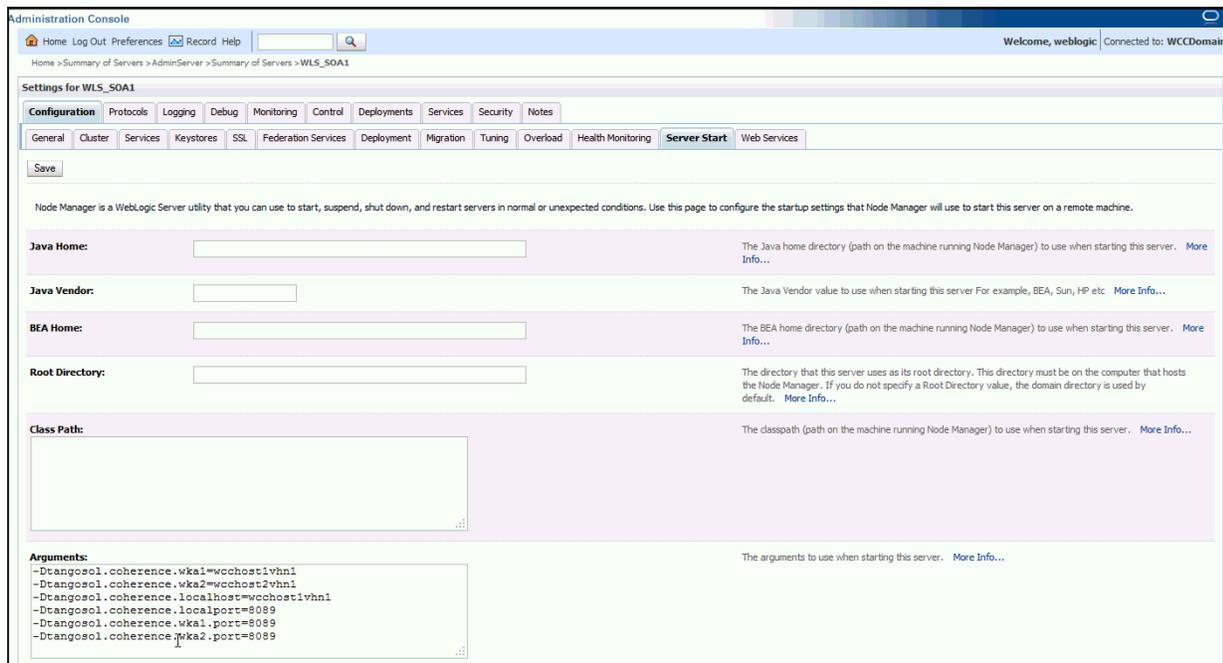
12.6 Completing Postconfiguration and Verification Tasks for Oracle SOA Suite

After extending the domain with the Configuration Wizard and configuring Oracle Coherence, follow these instructions for postconfiguration and validation. The following sections describe how to do postconfiguration and verification tasks for Oracle SOA Suite:

- Section 12.6.1, "Disabling Host Name Verification for the WLS_SOAn Managed Servers"

- Section 12.6.2, "Propagating the Domain Configuration to WLS_SOA1 and WLS_SOA2"

- Section 12.6.3, "Starting and Validating the WLS_SOA1 Managed Server"

- Section 12.6.4, "Starting and Validating the WLS_SOA2 Managed Server"

- Section 12.6.5, "Validating GridLink Data Sources for Oracle SOA Suite"

12.6.1 Disabling Host Name Verification for the WLS_SOA*n* 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. You must disable the host name verification for the WLS_SOA1 and WLS_SOA2 Managed Servers to avoid errors when managing the different WebLogic Server instances. For more information, see Section 8.4.5, "Disabling Host Name Verification."

You enable host name verification again once the enterprise deployment topology configuration is complete. For more information, see Section 16.3, "Enabling Host Name Verification Certificates for Node Manager."

12.6.2 Propagating the Domain Configuration to WLS_SOA1 and WLS_SOA2

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

To propagate the domain configuration to the Oracle SOA Suite Managed Servers:

1. Create a copy of the Managed Server domain directory and the Managed Server applications directory.

2. Run the following `pack` command on WCCHOST1 to create a template pack:

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

   ```
   ./pack.sh -managed=true -domain=ASERVER_HOME -template=edgdomaintemplateSOA.jar
   -template_name=edgdomain_templateSOA
   ```

   In the reference topology, `ORACLE_COMMON_HOME` is the `/u01/oracle/products/fmw_home/oracle_common` directory, and `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

3. Run the following `unpack` command on WCCHOST1 to propagate the template created in the preceding step to the WLS_SOA1 domain directory:

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

   ```
   ./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateSOA.jar -app_
   dir=APPLICATION_HOME -overwrite_domain=true
   ```

   In the reference topology, `MSERVER_HOME` is the `/u02/oracle/config/domains/WCCDomain` directory, and `APPLICATION_HOME` is the `/u01/oracle/config/applications/WCCDomain` directory.

   > **Notes:**
   >
   > - Make sure to run `unpack` from the `ORACLE_COMMON_HOME/common/bin/` directory, not from `WL_HOME/common/bin/`.
   >
   > - The `APPLICATION_HOME` directory gets backed up with this `unpack` command.
   >
   > - 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.

4. Run the following command on WCCHOST1 to copy the template pack created in step 2 to WCCHOST2:

   ```
   scp edgdomaintemplateSOA.jar oracle@WCCHOST2:ORACLE_COMMON_HOME/common/bin
   ```

5. Run the following `unpack` command on WCCHOST2 to unpack the propagated template to the WLS_SOA2 Managed Server domain directory:

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

   ```
   ./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateSOA.jar -app_
   dir=APPLICATION_HOME -overwrite_domain=true
   ```

> **Notes:**
>
> - Make sure to run `unpack` from the *ORACLE_COMMON_HOME*/common/bin/ directory, not from *WL_HOME*/common/bin/.
>
> - The *APPLICATION_HOME* directory gets backed up with this `unpack` command.

6. Restart the Administration Server to make these changes take effect, stopping it with the `nmKill` command, or with the Administration Console, and then starting it with the `nmStart` command, as described in Section 10.3, "Restarting the Administration Server." Log in to the Administration Console using the credentials for the `weblogic` user.

12.6.3 Starting and Validating the WLS_SOA1 Managed Server

You can start and validate the WLS_SOA1 Managed Server through the Administration Console.

To start the WLS_SOA1 Managed Server on WCCHOST1:

1. Log in to the Oracle WebLogic Server Administration Console at `http://admin.example.com:7001/console`.

2. Start the WLS_SOA1 Managed Server through the WebLogic Server Administration Console, as follows:

   a. Expand the **Environment** node in the **Domain Structure** tree on the left.

   b. Click **Servers**.

   c. On the Summary of Servers page, click the **Control** tab.

   d. Select **WLS_SOA1** from the **Servers** column of the table.

   e. Click **Start**.

3. 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. For possible causes, see Section 19.13, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology."

4. Access the following URLs:

   - Access `http://WCCHOST1VHN1:8001/soa-infra` to verify the status of WLS_SOA1.

   - Access `http://WCCHOST1VHN1:8001/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://WCCHOST1VHN1:8001/integration/worklistapp` to verify the status of the worklist application.

12.6.4 Starting and Validating the WLS_SOA2 Managed Server

After you start the WLS_SOA2 Managed Server, you can validate it by verifying its status through the WebLogic Server Administration Console and some URLs.

> **Note:** Before starting the WLS_SOA2 Managed Server using the WebLogic Server Administration Console, make sure Node Manager is running. Section 19.8.1, "Assumptions and Procedure," says to start it, in Step 3, "Start Node Manager in WCCHOST2."
>
> If Node Manager is not running, restart it on WCCHOST2, as described in Section 8.4.2, "Starting Node Manager on WCCHOST1."

To start and validate the WLS_SOA2 Managed Server:

1. Start the WLS_SOA2 Managed Server using the WebLogic Server Administration Console, as follows:

   a. Expand the Environment node in the **Domain Structure** tree on the left.

   b. Click **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 19.13, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology" for possible causes.

3. Access the following URLs:

   ■ Access `http://WCCHOST2VHN1:8001/soa-infra` to verify the status of WLS_SOA2.

   ■ Access `http://WCCHOST2VHN1:8001/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.

   ■ Access `http://WCCHOST2VHN1:8001/integration/worklistapp` to verify the status of the worklist application.

12.6.5 Validating GridLink Data Sources for Oracle SOA Suite

After the servers are started, verify that the GridLink data sources are correctly configured and that the ONS setup is correct. Perform this procedure for every GridLink data source created.

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.

5. Click the **Testing** tab (Figure 12–8), select one of the servers, and click **Test Data Source**.

Figure 12–8   Testing a GridLink Data Source for Oracle SOA Suite
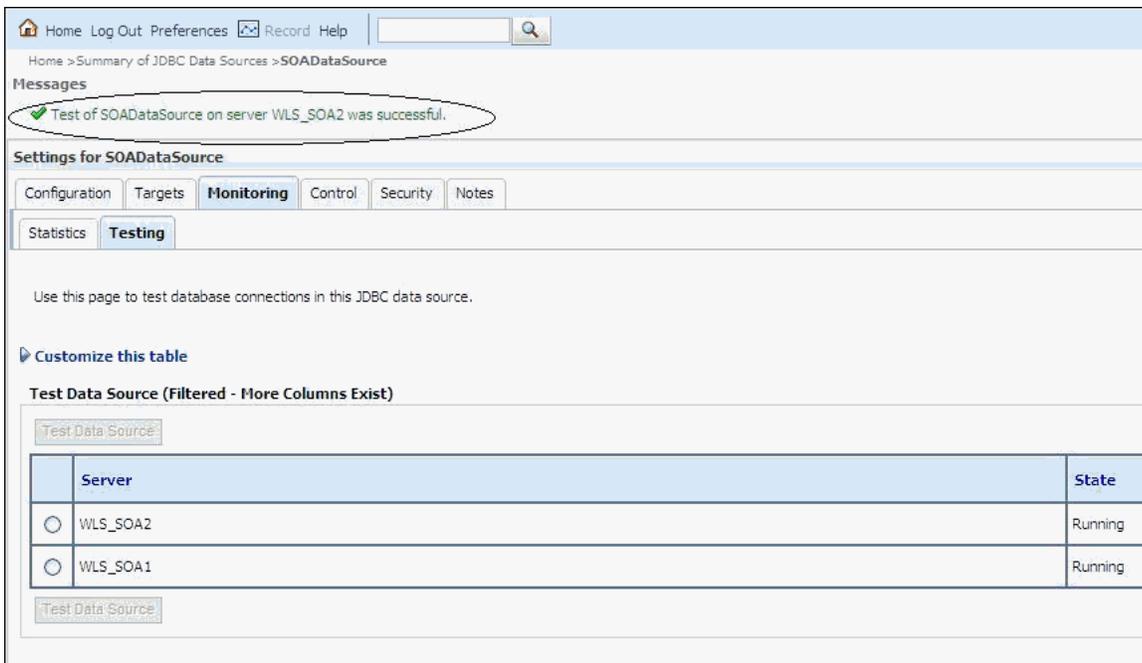
The test should be successful if the configuration is correct.

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. In the **Domain Structure** tree on the Administration Console, expand **Services**, then click **Data Sources**.

2. Click the name of a GridLink data source that was created.

3. Click the **Monitoring** tab.

4. Click the name of the server (WLS_SOA1).

5. Click the **ONS** tab and then the **Testing** tab (Figure 12–9).

6. Select a server, and click **Test ONS**.

Figure 12–9   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@WCCDBHOST1 ~]$ srvctl status scan_listener
SCAN Listener LISTENER_SCAN1 is enabled
SCAN listener LISTENER_SCAN1 is running on node WCCDBHOST1
SCAN Listener LISTENER_SCAN2 is enabled
SCAN listener LISTENER_SCAN2 is running on node WCCDBHOST2
SCAN Listener LISTENER_SCAN3 is enabled
SCAN listener LISTENER_SCAN3 is running on node WCCDBHOST2


[orcl@WCCDBHOST1 ~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016


[orcl@WCCDBHOST1 ~]$ srvctl status nodeapps | grep ONS
ONS is enabled
ONS daemon is running on node: WCCDBHOST1
ONS daemon is running on node: WCCDBHOST2
```

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

12.7 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, using the WebLogic Server Administration Console, 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 WebLogic Server Administrator user name, password, and server URL (t3://ADMINVHN:7001) 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 enterprise deployment environments (see the following text for the script input parameters):

```
Execfile("MW_HOME/oracle_common/bin/configure-joc.py").
Enter Hostnames (eg host1,host2) : WCCHOST1VHN1,WCCHOST2VHN1
.
Do you want to specify a cluster name (y/n) <y>y
.
Enter Cluster Name : SOA_Cluster
.
Enter Discover Port : 9991
.
Enter Distribute Mode (true|false) <true> : true
.
Do you want to exclude any server(s) from JOC configuration (y/n) <n> n
```

After configuring the Java Object Cache using WLST commands or the configure-joc.py script, restart all affected Managed Servers, using the WebLogic Server Administration Console, for the configurations to take effect.

Script Input Parameters

The input parameters are prompted by the script. The script can be used to perform the following optional 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>n
Enter Managed Server and Discover Port (eg WLS_SOA1:9991, WLS_SOA21:9991) :
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`.

12.8 Configuring Oracle HTTP Server with the Extended Domain

After propagating the domain configuration to WCCHOST2, configure the Oracle HTTP Server with the extended domain.

This section includes the following topics:

12.8.1 Configuring Oracle HTTP Server for the WLS_SOA Managed Servers

To enable Oracle HTTP Server to route to SOA_Cluster, which contains the WLS_
SOA*n* Managed Servers, you must set the WebLogicCluster parameter to the list of
nodes in the cluster.

To configure Oracle HTTP Server for the WLS_SOA Managed Servers:

1. For each of the web servers on WEBHOST1 and WEBHOST2, add the following
   lines to the *ORACLE_INSTANCE*/config/OHS/ohs1/moduleconf/wccinternal_
   vh.conf and *ORACLE_INSTANCE*/config/OHS/ohs2/moduleconf/wccinternal_
   vh.conf files:

```
# WSM-PM
<Location /wsm-pm>
    WebLogicCluster WCCHOST1VHN1:8001,WCCHOST2VHN1:8001
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# SOA soa-infra app
<Location /soa-infra>
    WebLogicCluster WCCHOST1VHN1:8001,WCCHOST2VHN1:8001
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# SOA inspection.wsil
<Location /inspection.wsil>
    WebLogicCluster WCCHOST1VHN1:8001,WCCHOST2VHN1:8001
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# Worklist
<Location /integration/>
    WebLogicCluster WCCHOST1VHN1:8001,WCCHOST2VHN1:8001
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# UMS prefs
<Location /sdpmessaging/userprefs-ui>
    WebLogicCluster WCCHOST1VHN1:8001,WCCHOST2VHN1:8001
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# Default to-do taskflow
<Location /DefaultToDoTaskFlow/>
    WebLogicCluster WCCHOST1VHN1:8001,WCCHOST2VHN1:8001
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>
```

```
# Workflow
<Location /workflow>
    WebLogicCluster WCCHOST1VHN1:8001,WCCHOST2VHN1:8001
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

#SOA Composer
<Location /soa/composer>
    WebLogicCluster WCCHOST1VHN1:8001,WCCHOST2VHN1:8001
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>
```

In the reference topology, *ORACLE_INSTANCE* is the `/u02/oracle/config/web1` or `/u02/oracle/config/web2` directory.

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

```
/u02/oracle/config/webN/bin/opmnctl restartproc ias-component=ohsX
```

For WEBHOST1, use `web1` for `ias-component` and for WEBHOST2 use `web2`.

The servers specified in the `WebLogicCluster` parameter are important only 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 *Oracle Fusion Middleware Using Web Server Plug-Ins with Oracle WebLogic Server Guide*.

12.8.2 Setting the Front-End HTTP Host and Port

You must set the front-end HTTP host and port for the Oracle WebLogic Server cluster hosting the Oracle SOA Suite servers.

To set the front-end HTTP host and port for the Oracle SOA Suite cluster:

1. Log in to the WebLogic Server Administration Console.

2. Go to the Change Center section and click **Lock & Edit**.

3. Expand the **Environment** node in the **Domain Structure** tree on the left.

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:** `wccinternal.example.com`

   - **Frontend HTTP Port:** `80`

8. Click **Save**.

9. Click **Activate Changes** in the Change Center section of the Administration Console.

10. Restart the WLS_SOA1 and WLS_SOA2 Managed Servers, using the WebLogic Server Administration Console, to make the front-end host directive in the cluster take effect.

12.8.3 Validating Access Through the Load Balancer

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. For possible causes, see Section 19.13, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology."

Validate access to `SOA_Cluster` using the following URLs:

- `http://wccinternal.example.com/soa-infra`

- `http://wccinternal.example.com/integration/worklistapp`

- `http://wccinternal.example.com/sdpmessaging/userprefs-ui`

- `http://wccinternal.example.com/soa/composer`

- `http://wccinternal.example.com/wsm-pm`

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

12.9 Configuring a Default Persistence Store for Transaction Recovery

Each server has a transaction log that stores information about the committed transactions 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 logs in a location accessible to each server and its backup servers.

> **Note:** The recommended location is on a dual-ported SCSI disk or on a Storage Area Network (SAN).

To set the locations of the default persistence stores for the Oracle SOA Suite Managed Servers:

1. Log in to the WebLogic Server Administration Console.

2. In the Change Center section of the page, click **Lock & Edit**.

3. In the **Domain Structure** tree on the left, expand the **Environment** node, and then click the **Servers** node.

4. On the Summary of Servers page, click the name of the server WLS_SOA1 (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.

5. On the **Configuration** tab, click the **Services** tab (not the top-level **Services** tab).

6. In the Default Store section of the page, enter the path to the folder where the default persistence store will store its data files. The directory structure of the path follows:

   ```
   ASERVER_HOME/SOA_Cluster/tlogs/
   ```

   In the reference topology, `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

7. Repeat steps 4, 5, and 6 for the WLS_SOA2 server.

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

9. Restart the WLS_SOA1 and WLS_SOA2 Managed Servers, using the WebLogic Server Administration Console.

10. After WLS_SOA1 and WLS_SOA2 are restarted, verify that the following `DAT` files are created in this directory:

    ```
    ASERVER_HOME/SOA_Cluster/tlogs/
    ```

    - `_WLS_WLS_SOA1000000.DAT`
    - `_WLS_WLS_SOA2000000.DAT`

    Note: To enable migration of the Transaction Recovery Service, specify a location on a persistent storage solution that is available to other servers in the cluster. Both WLS_SOA1 and WLS_SOA2 must be able to access this directory. Also, the directory must exist before you restart the servers.

12.10 Configuring Node Manager for the WLS_SOA Managed Servers

Oracle recommends using host name verification for 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. For more details, see Chapter 16, "Setting Up Node Manager for an Enterprise Deployment." The procedures in that chapter must be performed for the Oracle WebCenter Content deployment.

The procedures in Section 16.3, "Enabling Host Name Verification Certificates for Node Manager," must be performed for the hosts and Oracle SOA Suite Managed Servers in the following table.

Host Name (*HOST*)	Virtual IP Address (*VIP*)	Server Name (*WLS_SERVER*)
WCCHOST1	WCCHOST1VHN1	WLS_SOA1
WCCHOST2	WCCHOST2VHN1	WLS_SOA2

For server migration of Oracle SOA Suite Managed Servers, you need to associate these servers with the specified virtual host names. Check that these virtual host names are enabled by DNS or /etc/hosts resolution in your system and that they map to the appropriate virtual IP addresses. For more information, see Section 3.4, "IP Addresses and Virtual IP Addresses."

12.11 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 WCCHOST1 and WCCHOST2 nodes. See Chapter 17, "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*: WCCHOST1
  - *HOST2*: WCCHOST2
- Cluster name:
  - *CLUSTER*: SOA_Cluster

12.12 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 *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. For information about database backup, see the *Oracle Database Backup and Recovery Guide*.

To back up the installation at this point:

1. Back up Oracle Web Tier on WEBHOST1:

   a. Shut down the instance using `opmnctl`:

   ```
   /u02/oracle/config/webN/bin/opmnctl stopall
   ```

   b. Back up the Middleware home for Oracle Web Tier with the following command (as root):

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

   c. Back up the Oracle instance for Oracle Web Tier with the following command:

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

   d. Start the instance with `opmnctl`:

   ```
   cd /u02/oracle/config/webN/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 /u01/oracle/config/domains/WCCDomain directory. Run the following command on WCCHOST1 to create the backup:

   ```
   tar -cvpf edgdomainback.tar /u01/oracle/config/domains/WCCDomain
   ```

13

Extending the Domain to Include Imaging

This chapter describes how to extend a domain with Oracle WebCenter Content: Imaging, using the Fusion Middleware Configuration Wizard.

This chapter includes the following sections:

- Section 13.1, "Overview of Extending the Domain to Include Imaging"
- Section 13.2, "Enabling VIP4 on WCCHOST1 and VIP5 on WCCHOST2"
- Section 13.3, "Extending the Domain with Imaging"
- Section 13.4, "Restarting the Administration Server"
- Section 13.5, "Completing Postconfiguration and Verification Tasks for Imaging"
- Section 13.6, "Configuring Oracle HTTP Server with the Imaging Cluster"
- Section 13.7, "Configuring Node Manager for the WLS_IMG Managed Servers"
- Section 13.8, "Configuring Server Migration for the WLS_IMG Managed Servers"
- Section 13.9, "Backing Up the Installation"

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

13.1 Overview of Extending the Domain to Include Imaging

The Imaging system is installed using the `WL_HOME` and `ORACLE_HOME` locations created in Chapter 7, "Installing the Software for an Enterprise Deployment," on a shared storage.

Extend the domain to include Imaging. Table 13–1 lists the steps for configuring Imaging and other tasks required for extending the domain with Imaging Managed Servers.

Table 13–1 Steps for Extending the Domain with Imaging

Step	Description	More Information
Prepare for extending the domain for Imaging	Enable a virtual IP address mapping for each of the host names for the Imaging WebLogic Server cluster.	Section 13.2, "Enabling VIP4 on WCCHOST1 and VIP5 on WCCHOST2"
Extend the domain for Imaging	Extend the domain you created in Chapter 8, "Creating a Domain for an Enterprise Deployment," with Oracle WebCenter Content: Imaging.	Section 13.3, "Extending the Domain with Imaging"
Disable host name verification for Imaging	Disable host name verification while setting up and validating the topology.	Section 13.5.1, "Disabling Host Name Verification for the WLS_IMG Managed Servers"
Propagate the domain configuration to the Imaging Managed Servers	Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the Managed Server domain directories.	Section 13.5.2, "Propagating the Domain Configuration to WLS_IMG1 and WLS_IMG2"
Configure JMS persistence stores	Configure the location for the JMS persistence stores as a directory that is visible to both Imaging Managed Servers.	Section 13.5.3, "Configuring JMS Persistence Stores for Imaging"
Restart the Administration Server for the domain	Stop and then restart the Administration Server.	Section 13.4, "Restarting the Administration Server"
Start the Imaging Managed Servers	Start the WLS_IMG1 and WLS_IMG2 Managed Servers.	Section 13.5.4, "Starting the Imaging Managed Servers"
Verify the configuration of GridLink data sources and Oracle Notification Service (ONS)	Follow these instructions to verify that the configuration of GridLink data sources and ONS is correct.	Section 13.5.5, "Validating GridLink Data Sources for Imaging"
Configure System MBeans for Imaging	Configure the `InputDirectories`, `SampleDirectory`, and `GDFontPath` MBeans in the System MBean Browser.	Section 13.5.7, "Configuring System MBeans for Imaging"
Enable the Imaging feature set in WebCenter Content	Enable the **IpmRepository** component of Oracle WebCenter Content Server.	Section 13.5.8, "Enabling the Imaging Feature Set in Oracle WebCenter Content"
Configure the Imaging Viewer Cache	Set the Imaging viewer to use cached documents.	Section 13.5.9, "Configuring the Imaging Viewer Cache"
Encrypt cached documents	Encrypt cached documents if additional security is required.	Section 13.5.10, "Encrypting Cached Documents"
Add the listen addresses for the Imaging Managed Servers	Add the host names of the WLS_IMG1 and WLS_IMG2 Managed Servers (WCCHOST1VHN2 and WCCHOST2VHN2) to the `SocketHostNameSecurityFilter` parameter list.	Section 13.5.11, "Adding the Imaging Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content"
Create a connection between the Imaging and WebCenter Content Managed Servers	Create a connection to Oracle WebCenter Content Server.	Section 13.5.12, "Creating a Connection to Content Server"
Configure the BPEL CSF credentials	Configure the required credentials to communicate with Oracle SOA Suite	Section 13.5.13, "Configuring a BPEL CSF Credential"
Configure a workflow connection for Imaging	Create and test a workflow connection.	Section 13.5.14, "Configuring a Workflow Connection"

Table 13–1   (Cont.) Steps for Extending the Domain with Imaging

Step	Description	More Information
Configure Oracle HTTP Server with the extended domain	Configure the Oracle HTTP Server with the Managed Servers, and set the WLS Cluster address for IMG_Cluster.	Section 13.6, "Configuring Oracle HTTP Server with the Imaging Cluster"
Validate access to WebCenter Content through Oracle HTTP Server	Verify the URLs to ensure that appropriate routing and failover is working from Oracle HTTP Server to IMG_Cluster.	Section 13.6.2, "Validating Access Through the Load Balancer"
Configure host name verification for communication between Node Manager and the Managed Servers in the domain	Use certificates for the different addresses communicating with the Administration Server and other servers.	Section 13.7, "Configuring Node Manager for the WLS_IMG Managed Servers"
Configure server migration for the Imaging Managed Servers.	Specify the Imaging Managed Server names, host names, and cluster name for migration.	Section 13.8, "Configuring Server Migration for the WLS_IMG Managed Servers"
Back up the Imaging configuration	Back up the newly extended domain configuration.	Section 13.9, "Backing Up the Installation"

13.2 Enabling VIP4 on WCCHOST1 and VIP5 on WCCHOST2

The Imaging system uses virtual host names as the listen addresses for the Managed Servers on which Imaging is running. These virtual host names and corresponding virtual IP addresses are required to enable server migration for the Imaging component. If you have not previously done so, you must enable a virtual IP address mapping from VIP4 to WCCHOST1VHN2 on WCCHOST1 and from VIP5 to WCCHOST2VHN2 on WCCHOST2, and you must correctly resolve the host names in the network system used by the topology, with either DNS Server or `/etc/hosts` resolution.

To enable the virtual IP addresses, follow the procedure described in Section 6.6, "Enabling Virtual IP Addresses" if you have not yet completed it. These virtual IP addresses and virtual host names are required to enable server migration for the Imaging servers. You can configure server migration for the Imaging servers later for high availability purposes. For more information about configuring server migration, see Chapter 17, "Configuring Server Migration for an Enterprise Deployment."

13.3 Extending the Domain with Imaging

You can extend the domain created in Chapter 8, "Creating a Domain for an Enterprise Deployment", and then extended with WebCenter Content, Inbound Refinery, Capture, and Oracle SOA Suite, to include Oracle WebCenter Content: Imaging. The instructions in this section are based on the assumption that the Imaging deployment uses the same database service as the Oracle WebCenter Content deployment (`wccedg.example.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 for 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. Shut down all Managed Servers in the domain.

3. On WCCHOST1, 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
   ```

4. Start the Fusion Middleware Configuration Wizard:

   ```
   ./config.sh
   ```

5. On the Welcome screen, select **Extend an existing WebLogic domain**, and click **Next**.

6. On the Select a WebLogic Domain Directory screen, select the WebLogic Server domain directory (*ASERVER_HOME*), and click **Next**.

   In the reference topology, *ASERVER_HOME* is the `/u01/oracle/config/domains/WCCDomain` directory.

7. On the Select Extension Source screen (Figure 13–1), make these selections:

   - Select **Extend my domain automatically to support the following added products**.

   - Select these products:

     Oracle WebCenter Content: Imaging Viewer Cache

     Oracle WebCenter Content: Imaging

     (If you select one of the preceding products, the other one is automatically selected.)

     Notes:

     - AXF for BPEL is included in Imaging.

     - For information about including Oracle WebCenter Content: AXF for BPM in Imaging, see *Installing and Configuring Oracle WebCenter Content*.

     The following products are grayed out if they were selected when you created the domain (Section 8.3) or extended it for WebCenter Content (Section 10.2), Inbound Refinery (Section 11.2), or Oracle SOA Suite components (Section 12.3).

     * **Basic WebLogic Server Domain**

     * **Oracle SOA Suite**

     * **Oracle Universal Content Management - Inbound Refinery**

     * **Oracle Universal Content Management - Content Server**

     * **Oracle Enterprise Manager Plugin for IBR**

    *   **Oracle Enterprise Manager**

    *   **Oracle WSM Policy Manager**

    *   **Oracle JRF**

Figure 13–1   Select Extension Source Screen for Imaging
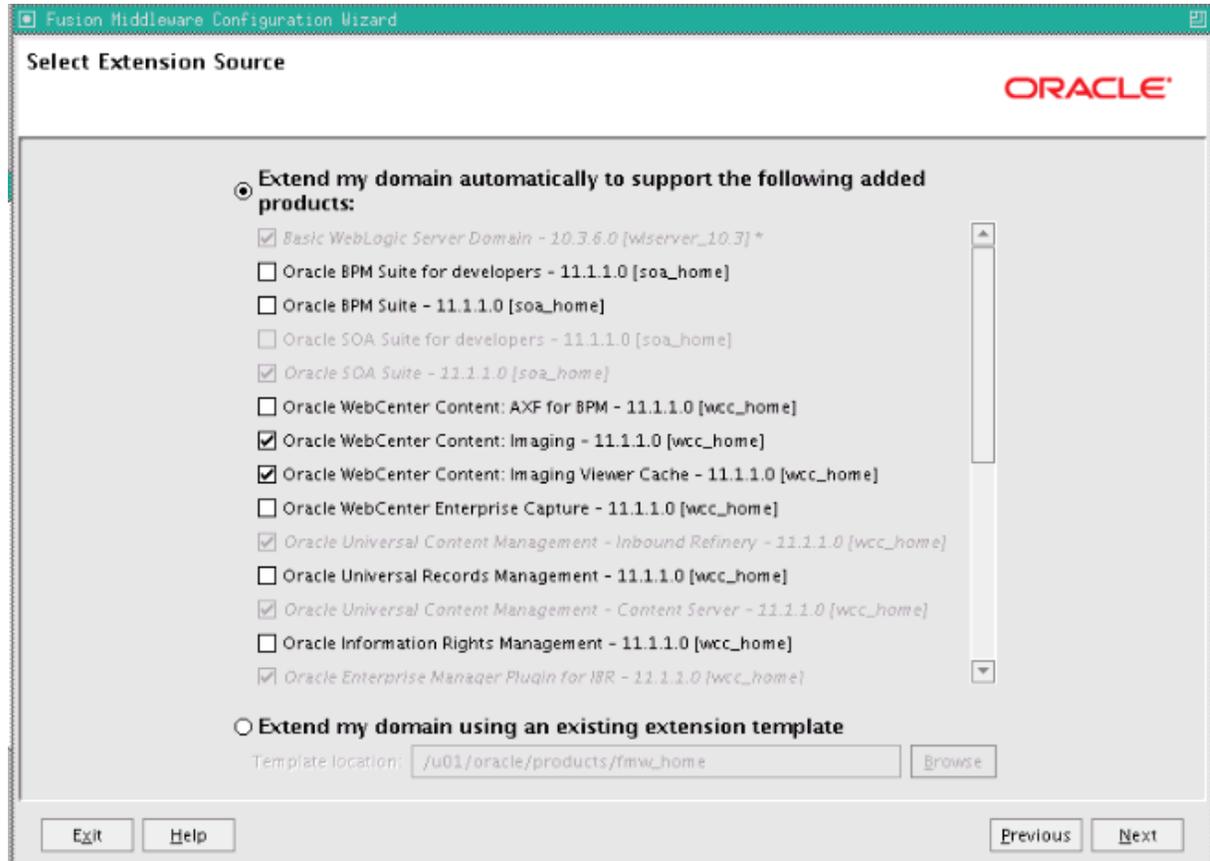
Click **Next**.

8. On the Configure JDBC Component Schema screen, which Figure 13–2 shows, perform the following steps:

    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 out.

Figure 13–2   Configure JDBC Component Schema Screen for Imaging
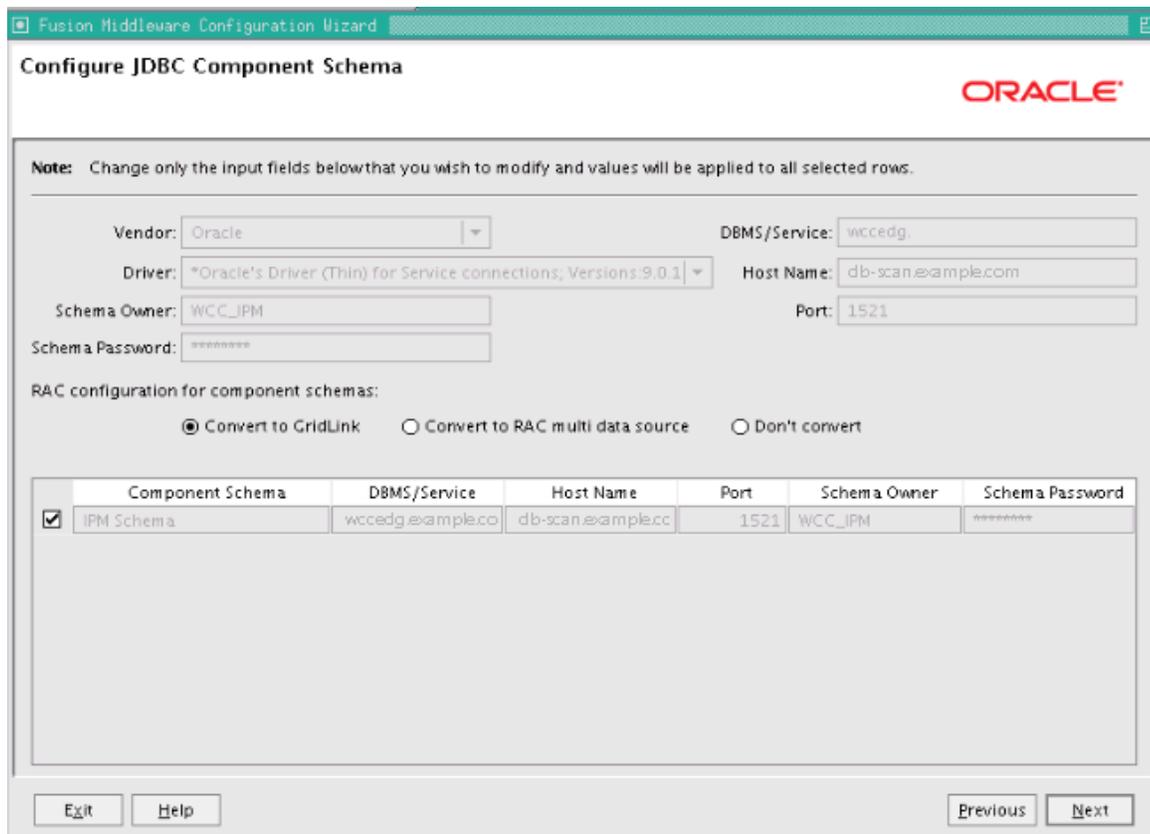
    c.   Click **Next**.

9. On the Configure GridLink RAC Component Schema screen (Figure 13–3), perform the following steps:

    a.   Make sure **IPM Schema** is selected. Leave the other data sources as they are.

Figure 13–3   Configure GridLink RAC Component Schema Screen for Imaging

b. Enter values for the following fields, specifying the connection information for the GridLink RAC database that was seeded through RCU:

– **Driver:** Select **Oracle's Driver (Thin) for GridLinkConnections; Versions: 11 and later**.

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

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

This book uses `WCC` 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>show parameter remote_listener;

NAME              TYPE      VALUE
-----             ------    -------
remote_listener   string    db-scan.example.com :1521
```

> **Note:** For Oracle Database 11*g* Release 1 (11.1), use the virtual IP address and port of each database instance listener, as in these examples:
>
> ```
> wccdbhost1-vip.example.com (port 1521)
>
> wccdbhost2-vip.example.com (1521)
> ```

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

```
[orcl@WCCDBHOST1 ~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016
```

> **Note:** For Oracle Database 11*g*, use the host name and port of each database's ONS service, as in these examples:
>
> ```
> wccdbhost1.example.com (port 6200)
>
> wccdbhost2.example.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.

10. On 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 13–4 Test JDBC Component Schema Screen for Imaging
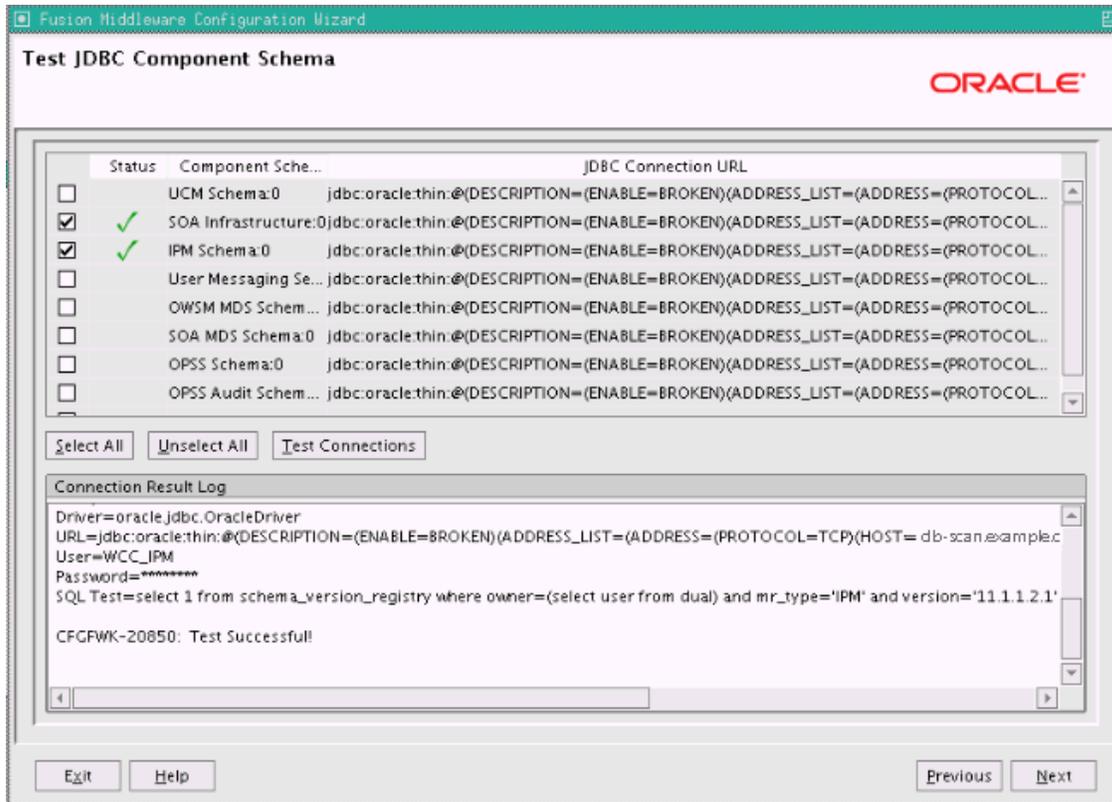
Click **Next** when the connection is successful.

11. On the Optional Configuration screen, select the following options:

    ■ **JMS Distributed Destination**

    ■ **Managed Servers, Clusters and Machines**

    ■ **Deployment and Services**

    Click **Next**.

12. On 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.

13. On 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 13–2. Do not modify the other servers that appear on this screen; leave them as they are.

Table 13–2 Managed Servers for Imaging

Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
WLS_IMG1	WCCHOST1VHN2	16000	n/a	No
WLS_IMG2	WCCHOST2VHN2	16000	n/a	No

Click **Next**.

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

Table 13–3   Cluster Configuration for Imaging

Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
IMG_Cluster	unicast	n/a	n/a	Leave empty.

Click **Next**.

15. On the Assign Servers to Clusters screen, add the following. Do not modify the other assignments that appear on this screen; leave them as they are.

- **IMG_Cluster:**
  - WLS_IMG1
  - WLS_IMG2

Click **Next**.

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

Table 13–4   Machines and Node Manager Listen Addresses

Name	Node Manager Listen Address
WCCHOST1	WCCHOST1
WCCHOST2	WCCHOST2
ADMINHOST	localhost

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

17. On the Assign Servers to Machines screen, assign servers to machines as follows:

- Assign **WLS_IMG1** to **WCCHOST1**.
- Assign **WLS_IMG2** to **WCCHOST2**.

Click **Next**.

18. On the Target Deployments to Clusters or Servers screen, make sure that targeting is done as follows (see Figure 13–5):

- The **usermessagingserver** and **usermessagingdriver-email** deployments are 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**.
- **EM Application** is targeted only to **AdminServer**.

Figure 13–5 Target Deployments to the Imaging Cluster
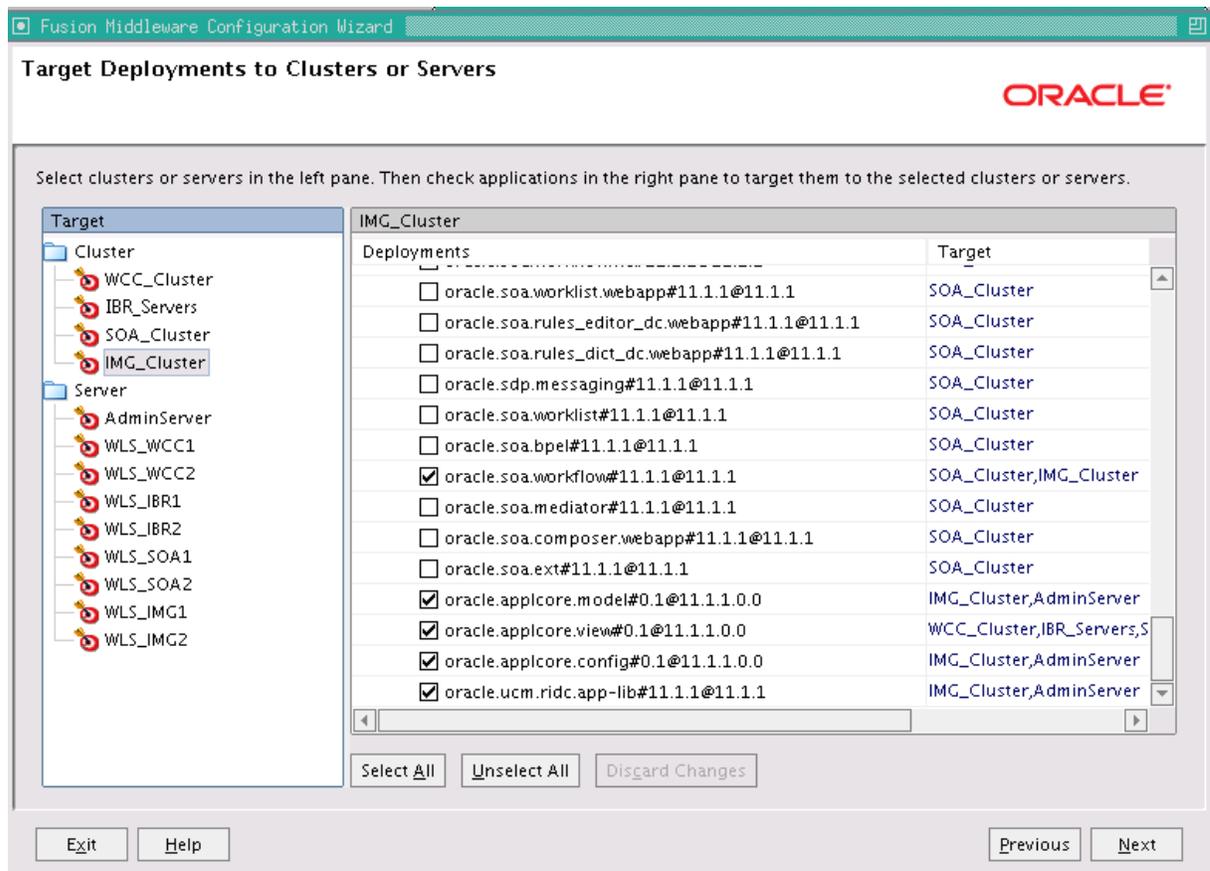
Click **Next**.

19. On the Target Services to Clusters or Servers screen, select all OPSS-related data sources to be targeted to **IMG_Cluster**:

- **opss-audit-viewDS**

- **opss-audit-DBDS**

- **opss-DBDS**

Click **Next**.

20. On the Configuration Summary screen, click **Extend**.

21. If a dialog box opens 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.

22. On the Creating Domain screen, click **Done**.

13.4 Restarting the Administration Server

You need to restart the Administration Server to make the domain extension changes take effect, using the Node Manager `nmKill` and `nmStart` commands through the Oracle WebLogic Scripting Tool (WLST), as described in Section 10.3, "Restarting the Administration Server." You can use the Administration Console instead of `nmKill` to stop the Administration Server.

13.5 Completing Postconfiguration and Verification Tasks for Imaging

The following sections describe how to do postconfiguration and verification tasks for Imaging:

- Section 13.5.1, "Disabling Host Name Verification for the WLS_IMG Managed Servers"
- Section 13.5.2, "Propagating the Domain Configuration to WLS_IMG1 and WLS_IMG2"
- Section 13.5.3, "Configuring JMS Persistence Stores for Imaging"
- Section 13.5.4, "Starting the Imaging Managed Servers"
- Section 13.5.5, "Validating GridLink Data Sources for Imaging"
- Section 13.5.6, "Validating Deployment of the Imaging Viewer Cache"
- Section 13.5.7, "Configuring System MBeans for Imaging"
- Section 13.5.8, "Enabling the Imaging Feature Set in Oracle WebCenter Content"
- Section 13.5.9, "Configuring the Imaging Viewer Cache"
- Section 13.5.10, "Encrypting Cached Documents"
- Section 13.5.11, "Adding the Imaging Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content"
- Section 13.5.12, "Creating a Connection to Content Server"
- Section 13.5.13, "Configuring a BPEL CSF Credential"
- Section 13.5.14, "Configuring a Workflow Connection"

13.5.1 Disabling Host Name Verification for the WLS_IMG 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 Imaging. You must disable the host name verification for the WLS_IMG1 and WLS_IMG2 Managed Servers to avoid errors when managing the different WebLogic Server instances. For more information, see Section 8.4.5, "Disabling Host Name Verification."

You enable host name verification again once the enterprise deployment topology configuration is complete. For more information, see Section 16.3, "Enabling Host Name Verification Certificates for Node Manager."

13.5.2 Propagating the Domain Configuration to WLS_IMG1 and WLS_IMG2

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

To propagate the domain configuration to the Imaging Managed Servers:

1. Create a copy of the Managed Server domain directory and the Managed Server applications directory.

2. Run the following `pack` command on WCCHOST1 to create a template pack:

    `cd ORACLE_COMMON_HOME/common/bin`

    `./pack.sh –managed=true –domain=ASERVER_HOME –template=edgdomaintemplateIMG.jar –template_name=edgdomain_templateIMG`

    In the reference topology, `ORACLE_COMMON_HOME` is the `/u01/oracle/products/fmw_home/oracle_common` directory, and `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

3. Run the following `unpack` command on WCCHOST1 to propagate the template created in the preceding step to the WLS_IMG1 domain directory:

    `cd ORACLE_COMMON_HOME/common/bin`

    `./unpack.sh –domain=MSERVER_HOME –template=edgdomaintemplateIMG.jar –app_dir=APPLICATION_HOME –overwrite_domain=true`

    In the reference topology, `MSERVER_HOME` is the `/u02/oracle/config/domains/WCCDomain` directory, and `APPLICATION_HOME` is the `/u01/oracle/config/applications/WCCDomain` directory.

    > **Notes:**
    >
    > - Make sure to run `unpack` from the `ORACLE_COMMON_HOME/common/bin` directory, not from `WL_HOME/common/bin`.
    >
    > - The `APPLICATION_HOME` directory gets backed up with this `unpack` command.
    >
    > - 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.

4. Run the following command on WCCHOST1 to copy the template pack created in step 1 to WCCHOST2:

    `scp edgdomaintemplateIMG.jar oracle@WCCHOST2: /u01/oracle/products/fmw_home/oracle_common/common/bin`

5. Run the following `unpack` command on WCCHOST2 to unpack the propagated template to the WLS_IMG2 Managed Server domain directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=/u02/oracle/config/domains/WCCDomain
-template=edgdomaintemplateIMG.jar -app_
dir=/u01/oracle/config/applications/WCCDomain -overwrite_domain=true
```

> **Notes:**
>
> - Make sure to run `unpack` from the *ORACLE_COMMON_HOME*/common/bin/ directory, not from *WL_HOME*/common/bin/.
>
> - The *APPLICATION_HOME* directory gets backed up with this `unpack` command.

6. Restart the Administration Server to make these changes take effect, stopping it with the `nmKill` command, or with the Administration Console, and then starting it with the `nmStart` command, as described in Section 10.3, "Restarting the Administration Server." Log in to the Administration Console using the credentials for the `weblogic` user.

13.5.3 Configuring JMS Persistence Stores for 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 WebLogic Server store (/u01/oracle/config/applications/WCCDomain/servers/*server_name*/data/store/default.).

To change the Imaging JMS server persistence store to use a shared base directory:

1. Log in to the WebLogic Server Administration Console.

2. In the **Domain Structure** tree on the left, expand the **Services** node, and then click the **Persistence Stores** node.

3. On the Summary of Persistence Stores page, click **Lock & Edit**.

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 (/u01/oracle/config/domains/WCCDomain/IMG_Cluster/jms).

6. Click **OK** and activate the changes.

7. In the **Domain Structure** tree on the left, expand the **Services** node, and then click the **Messaging->JMS Servers** node.

8. On the Summary of JMS Servers page, click **IpmJmsServer1 JMS Server** (represented as a hyperlink) in the **Name** column of the table.

9. On the settings page for the JMS server, click **Lock & Edit**.

10. In the **Persistent Store** drop-down list, select **IMGJMSServer1Store**.

11. Click **Save and Activate**.

12. Repeat the steps and create **IMGJMSServer2Store** for IpmJmsServer2.

13.5.4 Starting the Imaging Managed Servers

Start the Imaging Managed Servers on WCCHOST1 and WCCHOST2.

To start the Imaging Managed Servers:

1. Start the WLS_IMG1 Managed Server:

   a. Log in to the WebLogic Server Administration Console at
      `http://ADMINVHN:7001/console`.

   b. In the **Domain Structure** tree on the left, 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://WCCHOST1VHN2:16000/imaging` to verify the status of WLS_IMG1.
   The Oracle WebCenter Content: Imaging login page opens. Enter your WebLogic
   Server administration user name and password to log in.

3. Start the WLS_IMG2 Managed Server:

   a. Log in to the WebLogic Server Administration Console at
      `http://ADMINVHN:7001/console`.

   b. In the **Domain Structure** tree on the left, 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://WCCHOST2VHN2:16000/imaging` to verify the status of WLS_IMG2.
   The Oracle WebCenter Content: Imaging login page opens. Enter your WebLogic
   Server administration user name and password to log in.

> **Note:**   These instructions are based on the assumption that the host
> name verification displayed previously for the Oracle WSM or Oracle
> SOA Suite Managed Servers in WCCHOST2 and that the Node
> Manager is already running on WCCHOST2.

13.5.5 Validating GridLink Data Sources for Imaging

After the servers are started, verify that the GridLink data sources are correctly
configured and that the ONS setup is correct. Perform this procedure for every
GridLink data source created.

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.

5. Click the **Testing** tab (Figure 13–6), select one of the servers, and click **Test Data
   Source**.

Figure 13–6   Testing a GridLink Data Source for Imaging
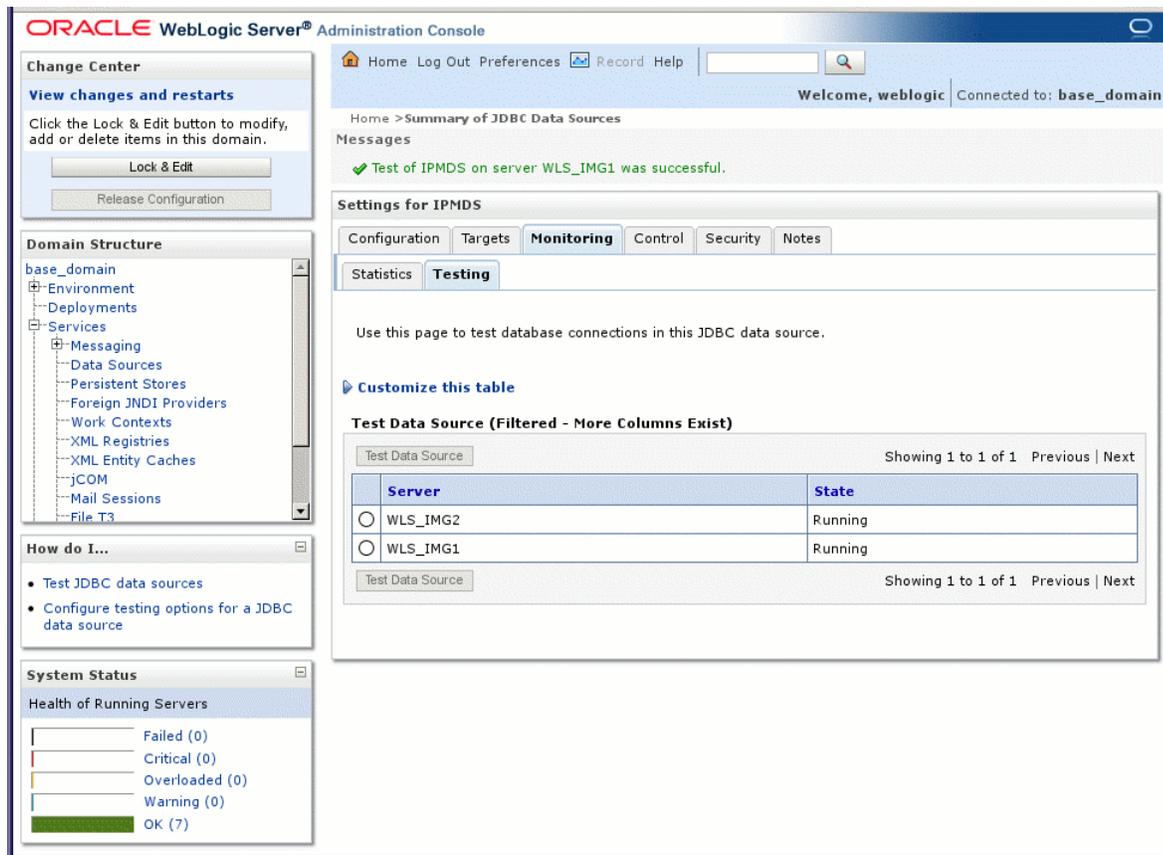
The test should be successful if the configuration is correct.

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 Imaging:

1. In the **Domain Structure** tree on the Administration Console, expand **Services**, then click **Data Sources**.

2. Click the name of a GridLink data source.

3. Click the **Monitoring** tab.

4. Click the name of the server (`WLS_IMG1`).

5. Click the **ONS** tab and then the **Testing** tab (Figure 13–7).

6. Select a server, and click **Test ONS**.

Figure 13–7   Testing the ONS Configuration for Imaging

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@WCCDBHOST1 ~]$ srvctl status scan_listener
SCAN Listener LISTENER_SCAN1 is enabled
SCAN listener LISTENER_SCAN1 is running on node WCCDBHOST1
SCAN Listener LISTENER_SCAN2 is enabled
SCAN listener LISTENER_SCAN2 is running on node WCCDBHOST2
SCAN Listener LISTENER_SCAN3 is enabled
SCAN listener LISTENER_SCAN3 is running on node WCCDBHOST2


[orcl@WCCDBHOST1 ~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016


[orcl@WCCDBHOST1 ~]$ srvctl status nodeapps | grep ONS
ONS is enabled
ONS daemon is running on node: WCCDBHOST1
ONS daemon is running on node: WCCDBHOST2
```

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

13.5.6 Validating Deployment of the Imaging Viewer Cache

After the Imaging servers are started, verify that the Viewer Cache was deployed correctly.

To validate deployment of the Imaging Viewer Cache:

1. In the WebLogic Server Administration Console, click **Deployments** under Domain Structure on the left.

2. In the `imaging-vc` row of the **Deployments** table, confirm that the **State** value is `Active` and the **Health** value is `OK`.

   If the **State** or **Health** value is different for `imaging-vc`, you need to redeploy the feature before proceeding.

13.5.7 Configuring System MBeans for Imaging

You can configure the following system MBeans for Imaging:

- `InputDirectories`

- `SampleDirectory`

- `GDFontPath`

To configure system MBeans for Imaging:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN:7001/em` (Figure 13–8).

Figure 13–8 System MBean Browser
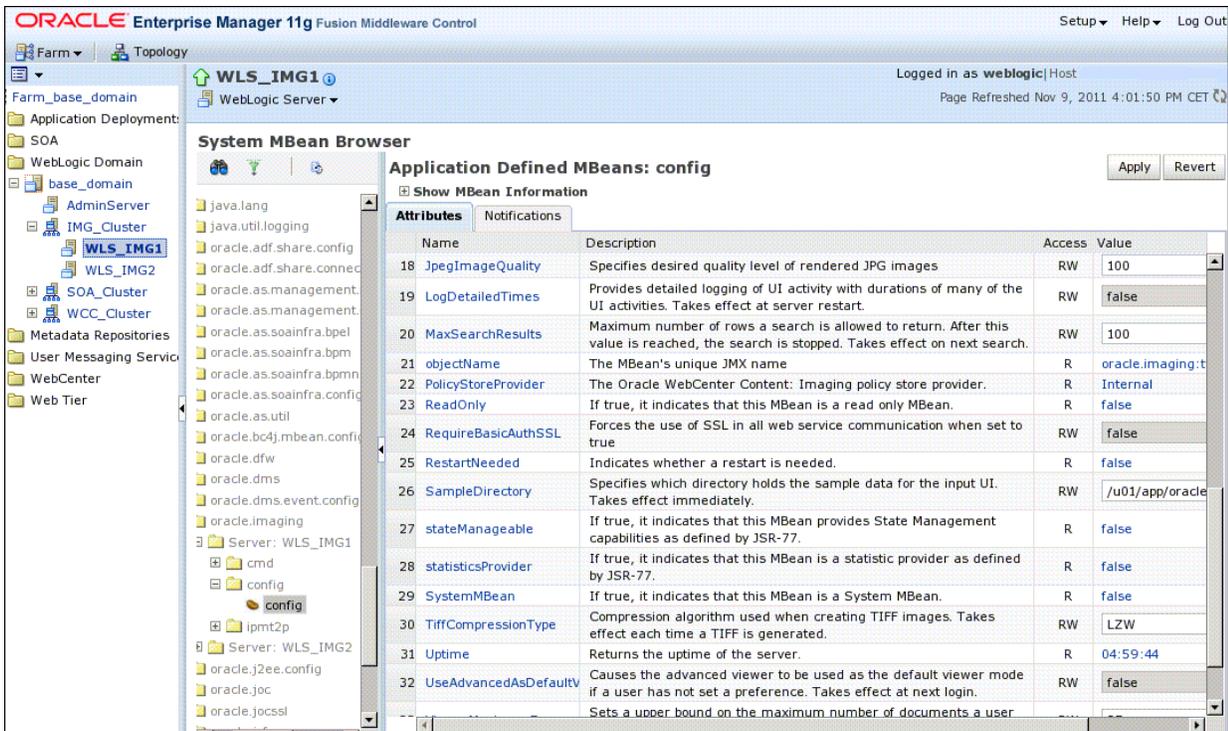
2. In the navigation tree on the left, expand the farm domain name, then **WebLogic Domain**, then the domain name, then **IMG_Cluster**, and then **WLS_IMG1**.

3. At the top, 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. On the right, set the **InputDirectories** MBean to specify the path to the input files: `ASERVER_HOME`/IMG_Cluster/input_files.

   In the reference topology, `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

   All Oracle WebCenter Content servers involved must be able to resolve this location (that is, through the NFS mount point).

8. Set the **SampleDirectory** MBean: `ASERVER_HOME`/IMG_Cluster/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 System. Check with your system administrator. The default is likely `/usr/share/X11/fonts/TTF` or `/usr/lib/X11/fonts/TTF`.

10. Validate that the changes are reflected on the 2nd Managed Server (WLS_IMG2). If not, add those changes to WLS_IMG2.

11. Click **Apply**.

13.5.8 Enabling the Imaging Feature Set in Oracle WebCenter Content

Enable the Imaging feature set in the Oracle WebCenter Content Server Component Manager.

To enable the Imaging feature set in Oracle WebCenter Content:

1. Log in to Content Server at `http://WCCHOST1:16200/cs`.

2. From the **Administration** tray or menu, choose **Admin Server**, then **Component Manager**.

3. On the Component Manager page, under **Integration**, select **IpmRepository**.

4. Click **Update** to enable the **IpmRepository** component, and confirm the action:

   a. In the paragraph at the top of the Component Manager page, click **advanced component manager**.

   b. On the Advanced Component Manager page, verify that **IpmRepository** is in the **Enabled Components** box.

5. Restart the Managed Server, as described in Section 8.4.3, "Starting the Administration Server on WCCHOST1," and then restart all Managed Servers in the Oracle WebCenter Content cluster, using the WebLogic Server Administration Console.

13.5.9 Configuring the Imaging Viewer Cache

The Imaging viewer can cache documents on the server outside of the repository to increase rendering speed on the client machine. Security for the cached documents is controlled by authentication for the server on which they are stored. If the server is considered secure, no additional security is necessary.

If additional security is required, you can encrypt cached documents, as described in Section 13.5.10, "Encrypting Cached Documents." For information about when to use the precache option and how to optimize ingestion and rendering when processing a large number of documents, see "Balancing Ingestion and Rendering When Viewer Cache is Enabled" in *Oracle Fusion Middleware Administering Oracle WebCenter Content: Imaging*.

To set the Imaging viewer to use cached documents, you need to set the following system MBeans:

- `ViewerCachePath`
- `ViewerCacheDays`
- `ViewerCacheEnablePrecache`

To configure these MBeans for the Imaging Viewer Cache, use the method described in Section 13.5.7, "Configuring System MBeans for Imaging," as follows:

- Set the **ViewerCachePath** MBean to the location where documents should be cached, and click **Apply**:

  ASERVER_HOME/IMG_Cluster/ViewerCache

  In the reference topology, *ASERVER_HOME* is the /u01/oracle/config/domains/WCCDomain directory.

  > **Note:** The **ViewerCachePath** MBean should be set to a location available to all servers in the cluster. If the directory path is not available to all servers, then each server will cache documents locally, resulting in multiple instances of the entire cache.

- Set the **ViewerCacheDays** MBean to 30, and click **Apply**.

  > **Note:** This configuration value specifies the number of days cached images should be retained before they are purged from the cache. Setting **ViewerCacheDays** equal to 0 prevents the cache from being purged.

- Set the **ViewerCacheEnablePrecache** MBean to true, and click **Apply**.

  > **Note:** This configuration value specifies whether documents should be cached as soon as they are ingested into Imaging (precached).

- If you are going to encrypt cached document, configure Imaging to encrypt them, as Section 13.5.10, "Encrypting Cached Documents," describes.

> **Note:** This is an additional option to encrypt the page images in the cache. The password credential must exist on the domain before you set the **ViewerCacheEnableEncryption** MBean. To add a password credential, use the method described in Section 13.5.10, "Encrypting Cached Documents."

For information about moving the viewer cache to a new location, see "Changing the Viewer Cache Path" in *Installing and Configuring Oracle WebCenter Content*.

13.5.10 Encrypting Cached Documents

If additional security is required, you can configure Imaging to encrypt cached documents. Encryption makes additional processing necessary to decrypt a document for viewing and reduces rendering speed. Even if Imaging is configured to encrypt the cached documents, there is a brief period of time during caching when generated documents are not encrypted.

To enable encryption of cached documents, add a new password credential to the domain through Oracle Enterprise Manager Fusion Middleware Control, and set the **ViewerCacheEnableEncryption** MBean.

To enable encryption of cached documents:

1. Log in to Fusion Middleware Control at `http://ADMINVHN:7001/em` (Figure 13–8).

2. Select the WebLogic Server domain for Oracle WebCenter Content.

3. From the **WebLogic Domain** menu, choose **Security** and then **Credentials**.

4. Select the map **oracle.imaging**. If no map named `oracle.imaging` exists, click **Create Map**, enter `oracle.imaging` for the map name, and then select it.

5. On the `oracle.imaging` map, click **Create Key**. Name the key `viewer.cache`, and select the type **Password**.

6. Enter a user name. The user name does not need to exist in any system.

7. Enter a password, confirm it, and then click **OK**.

8. Set the **ViewerCacheEnableEncryption** MBean to `true`, as described in Section 13.5.7, "Configuring System MBeans for Imaging."

For information about disabling encryption, see "Disabling Encryption of Cached Documents" in *Installing and Configuring Oracle WebCenter Content*.

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

Add the host names of the WLS_IMG1 and WLS_IMG2 Managed Servers (WCCHOST1VHN2 and WCCHOST2VHN2, respectively) to the `SocketHostNameSecurityFilter` parameter list.

To add the Imaging server listen addresses to allowed hosts in Oracle WebCenter Content:

1. Open the file `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs/config/config.cfg` in a text editor.

2. Remove or comment out the following line:

   ```
   SocketHostAddressSecurityFilter=127.0.0.1|WCCHOST1-IP|WCCHOST2-IP|WEBHOST1-IP|WEBHOST2-IP
   ```

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

   ```
   SocketHostNameSecurityFilter=localhost|localhost.example.com|WEBHOST1|WEBHOST2|WCCHOST1|WCCHOST2|WCCHOST1VHN1|WCCHOST2VHN1|WCCHOST1VHN2|WCCHOST2VHN2|ucminternal.example.com|load-balancer-host-name
   AlwaysReverseLookupForHost=Yes
   ```

   > **Notes:**
   >
   > - You can use IP addresses (listen addresses) in the value of `SocketHostAddressSecurityFilter`, as suggested in Section 19.13.13, "Improving Performance with Very Intensive Document Uploads from Oracle WebCenter Content: Imaging to Oracle WebCenter Content."
   >
   > - The load balancer host name is the one that was used to configure the virtual servers in Section 3.3, "Load Balancers."

4. Save the modified `config.cfg` file, and restart the Oracle WebCenter Content servers, using the WebLogic Server Administration Console, for the changes to take effect.

13.5.12 Creating a Connection to Content Server

Create a connection to Oracle WebCenter Content Server connection in Imaging.

To create a Content Server connection:

1. Log in to the WLS_IMG1 Imaging console at `http://WCCHOST1VHN2:16000/imaging`.

2. On the left, click **Manage Connections**, and then **Create Content Server Connection**.

3. Enter a name and description for the new connection, and then click **Next**.

4. On the Connection Settings screen, make these changes:

   - Unselect **Use Local Content Server**.

   - Set the Content Server port to 6300.

   - Add the `ucminternal.example.com` load balancer address under **Content Server Pool**.

If you get a `Permission denied` error, go back to Section 13.5.11, "Adding the Imaging Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content," and add name of the host that was denied to the list of allowable hosts.

Click **Next**.

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

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

13.5.13 Configuring a BPEL CSF Credential

When connecting to a BPEL system from Oracle WebCenter Content: Imaging, you need to configure the required credential to communicate with Oracle SOA Suite.

To add a BPEL CSF credential:

1. On WCCHOST1, change the directory to the `common/bin/` location under the WebCenter Content Oracle home in WCCHOST1 (where your Administration Server resides):

   ```
   cd WCC_ORACLE_HOME/common/bin
   ```

   (*WCC_ORACLE_HOME* is the Oracle home for Oracle WebCenter Content, which is *MW_HOME*/wcc_home 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, 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` value in the command is the *alias*, which is used for the `Credential Alias` property of the BPEL connection definition in the Imaging administration user interface (also the `Connection.CONNECTION_BPEL_CSFKEY_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.

   > **Note:** A new map will need to be created or the existing one updated if a different user or password, or both, is later used when integrating the Oracle SOA Suite system with a central LDAP and single sign-on (SSO) system. For details on the sample users created, see Chapter 18, "Integrating with Oracle Identity Management."

5. Restart the Oracle SOA Suite and Imaging Managed Servers, using the WebLogic Server Administration Console.

13.5.14 Configuring a Workflow Connection

Create and test a workflow connection for Imaging.

To configure a workflow connection:

1. Log in to the WLS_IMG1 imaging console at `http://WCCHOST1VHN2:16000/imaging`.

2. 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, perform the following steps:

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

    b. In the **Credential Alias** field, provide the credential alias created earlier, `basic.credential`, as described in Section 13.5.13, "Configuring a BPEL CSF Credential."

    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**.

13.6 Configuring Oracle HTTP Server with the Imaging Cluster

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.

This section includes the following topics:

- Section 13.6.1, "Configuring Oracle HTTP Server for the WLS_IMG Managed Servers"

- Section 13.6.2, "Validating Access Through the Load Balancer"

13.6.1 Configuring Oracle HTTP Server for the WLS_IMG Managed Servers

To configure Oracle HTTP Server for the WLS_IMG Managed Servers:

1. For each of the web servers on WEBHOST1 and WEBHOST2, add the following lines to the *ORACLE_INSTANCE*/config/OHS/ohs1/moduleconf/wcc_vh.conf and *ORACLE_INSTANCE*/config/OHS/ohs2/moduleconf/wcc_vh.conf files:

```
# Oracle WebCenter Content: Imaging Application
<Location /imaging >
    WebLogicCluster WCCHOST1VHN2:16000,WCCHOST2VHN2:16000
    SetHandler weblogic-handler
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>
```

2. For each of the web servers on WEBHOST1 and WEBHOST2, add the following lines to the *ORACLE_INSTANCE*/config/OHS/ohs1/moduleconf/wccinternal_vh.conf and *ORACLE_INSTANCE*/config/OHS/ohs2/moduleconf/wccinternal_vh.conf files:

```
# Oracle WebCenter Content: Imaging Application
<Location /imaging/ws >
    WebLogicCluster WCCHOST1VHN2:16000,WCCHOST2VHN2:16000
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# AXF WS Invocation
<Location /axf-ws >
    WebLogicCluster WCCHOST1VHN2:16000,WCCHOST2VHN2:16000
    SetHandler weblogic-handler
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>
```

In the reference topology, *ORACLE_INSTANCE* is the /u02/oracle/config/web1 or /u02/oracle/config/web2 directory.

> **Note:** Components such as Capture use these URIs over the internal load-balancer URL (wccinternal.example.com) for internal references, such as in a Capture profile configuration for Imaging.

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

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

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

13.6.2 Validating Access Through the Load Balancer

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

To verify the URLs:

1. While WLS_IMG2 is running, stop WLS_IMG1 from the WebLogic Server Administration Console.

2. Access `http://wcc.example.com/imaging` to verify that it is functioning properly. (You will not be able to retrieve reports or data because 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://wcc.example.com/imaging` to verify that it is functioning properly.

6. Start WLS_IMG2 from the WebLogic Server Administration Console.

13.7 Configuring Node Manager for the WLS_IMG Managed Servers

Oracle recommends using host name verification for 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. For more details, see Chapter 16, "Setting Up Node Manager for an Enterprise Deployment."

The procedures in that chapter must be performed for the Oracle WebCenter Content deployment. The procedures in Section 16.3, "Enabling Host Name Verification Certificates for Node Manager," must be performed for the hosts and Oracle SOA Suite Managed Servers in the following table.

Host Name (*HOST*)	Virtual IP Address (*VIP*)	Server Name (*WLS_SERVER*)
WCCHOST1	WCCHOST1VHN2	WLS_IMG1
WCCHOST2	WCCHOST2VHN2	WLS_IMG2

For server migration of the Imaging Managed Servers, you need to associate these servers with the specified virtual host names. Check that these virtual host names are enabled by DNS or `/etc/hosts` resolution in your system and that they map to the appropriate virtual IP addresses. For more information, see Section 3.4, "IP Addresses and Virtual IP Addresses."

13.8 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. For more details, see Chapter 17, "Configuring Server Migration for an Enterprise Deployment." For 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

13.9 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. For information about database backup, see the *Oracle Database Backup and Recovery User's Guide*.

To back up the installation at this point:

1. Back up Oracle Web Tier on WEBHOST1:

   a. Shut down the instance using `opmnctl`.

   ```
   /u02/oracle/config/webN/bin/opmnctl stopall
   ```

   b. Back up the Middleware home for Oracle Web Tier with the following command (as root):

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

   c. Back up the Oracle instance for Oracle Web Tier with the following command:

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

   d. Start the instance with `opmnctl`:

   ```
   cd /u02/oracle/config/webN/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 `/u01/oracle/config/domains/WCCDomain` directory. Run the following command in WCCHOST1 to create the backup:

   ```
   tar -cvpf edgdomainback.tar /u01/oracle/config/domains/WCCDomain
   ```

14

Extending the Domain to Include Capture

This chapter describes how to extend a domain with Oracle WebCenter Enterprise Capture using the Fusion Middleware Configuration Wizard.

This chapter includes the following sections:

- Section 14.1, "Overview of Extending the Domain to Include Capture"
- Section 14.2, "Enabling VIP6 on WCCHOST1 and VIP7 on WCCHOST2"
- Section 14.3, "Extending the Domain for Capture"
- Section 14.4, "Restarting the Administration Server"
- Section 14.5, "Completing Postconfiguration and Verification Tasks for Capture"
- Section 14.6, "Configuring Oracle HTTP Server for the Capture Cluster"
- Section 14.7, "Configuring Node Manager for the WLS_CPT Managed Servers"
- Section 14.8, "Configuring Server Migration for the WLS_CPT Managed Servers"
- Section 14.9, "Backing Up the Installation"

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

14.1 Overview of Extending the Domain to Include Capture

The Capture system is installed using the WebLogic Server home (*WL_HOME*) and Oracle home (*ORACLE_HOME*) locations created in Chapter 7, "Installing the Software for an Enterprise Deployment," on a shared storage.

Extend the domain to include Capture. Table 14–1 lists the steps for configuring Capture and other tasks required for extending the domain with Capture Managed Servers.

This configuration is only for the initial Capture setup. For more information about configuring Capture, such as Capture profiles, see *Oracle Fusion Middleware Administering Oracle WebCenter Enterprise Capture*.

Table 14–1   Steps for Extending the Domain with Capture

Step	Description	More Information
Prepare for extending the domain for Capture	Enable a virtual IP address mapping for each of the host names for the Capture WebLogic Server cluster.	Section 14.2, "Enabling VIP6 on WCCHOST1 and VIP7 on WCCHOST2"
Extend the domain for Capture	Extend the domain you created in Chapter 8, "Creating a Domain for an Enterprise Deployment."	Section 14.3, "Extending the Domain for Capture"
Propagate the domain configuration to the Capture Managed Servers	Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the Managed Server domain directories.	Section 14.5.2, "Propagating the Domain Configuration to WLS_CPT1 and WLS_CPT2"
Configure JMS persistence stores	Configure the location for the JMS persistence stores as a directory that is visible to both Capture Managed Servers.	Section 14.5.5, "Configuring JMS Persistence Stores for Capture"
Start the Capture Managed Servers	Start the WLS_CPT1 and WLS_CPT2 Managed Servers.	Section 14.5.3.2, "Starting the Capture Managed Servers"
Verify the configuration of GridLink data sources and Oracle Notification Service (ONS)	Follow these instructions to verify that the configuration of GridLink data sources and ONS is correct.	Section 14.5.4, "Validating GridLink Data Sources for Capture"
Add the listen addresses for the Capture Managed Servers	Add the host names of the WLS_CPT1 and WLS_CPT2 Managed Servers (WCCHOST1VHN3 and WCCHOST2VHN3) to the `SocketHostNameSecurityFilter` parameter list.	Section 14.5.6, "Adding the Capture Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content"
Complete the Capture configuration	Complete the initial configuration of Capture and performing other postinstallation tasks.	Section 14.5.3, "Completing the Initial Capture Configuration"
Configure Oracle HTTP Server with the extended domain	Configure the Oracle HTTP Server with the Managed Servers, and set the WLS Cluster address for CPT_Cluster.	Section 14.6, "Configuring Oracle HTTP Server for the Capture Cluster"
Set the front-end HTTP host and port for Capture.	Configure the front-end HTTP host and port for CPT_Cluster.	Section 14.6.2, "Setting the Front-End HTTP Host and Port"
Validate access to WebCenter Content through Oracle HTTP Server	Verify the URLs to ensure that appropriate routing and failover is working from Oracle HTTP Server to CPT_Cluster.	Section 14.6.3, "Validating Access Through the Load Balancer"
Configure Node Manager for Capture	Specify the Capture Managed Server names, host names, and cluster name for migration.	Section 14.7, "Configuring Node Manager for the WLS_CPT Managed Servers"
Configure server migration for the Capture Managed Servers.	Specify the Capture Managed Server names, host names, and cluster name for migration.	Section 14.8, "Configuring Server Migration for the WLS_CPT Managed Servers"
Back up the Capture configuration	Back up the newly extended domain configuration.	Section 14.9, "Backing Up the Installation"

14.2 Enabling VIP6 on WCCHOST1 and VIP7 on WCCHOST2

The Capture system uses virtual host names as the listen addresses for the Managed Servers on which Capture is running. These virtual host names and corresponding virtual IP addresses are required to enable server migration for the Capture component. If you have not previously done so, you must enable a virtual IP address mapping from VIP6 to WCCHOST1VHN3 on WCCHOST1 and from VIP7 to WCCHOST2VHN3 on WCCHOST2, and you must correctly resolve the host names in the network system used by the topology, with either DNS Server or `/etc/hosts` resolution.

To enable the virtual IP addresses, follow the procedure described in Section 6.6, "Enabling Virtual IP Addresses" if you have not yet completed it. These virtual IP addresses and virtual host names are required to enable server migration for the Capture servers. You can configure server migration for the Capture servers later for high availability purposes. For more information about configuring server migration, see Chapter 17, "Configuring Server Migration for an Enterprise Deployment."

14.3 Extending the Domain for Capture

You extend the domain configured in Chapter 10, "Extending the Domain to Include WebCenter Content," to include Oracle WebCenter Enterprise Capture. The instructions in this section are based on the assumption that the Capture deployment uses the same database service as the Oracle WebCenter Content deployment (`wccedg.example.com`). However, a deployment can choose to use a different database service specifically for Capture.

> **Note:** Before performing these steps, back up the domain as described in the *Oracle Fusion Middleware Administrator's Guide*.

To extend the domain for Capture:

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. Shut down all Managed Servers in the domain.

3. On WCCHOST1, 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
   ```

4. Start the Fusion Middleware Configuration Wizard:

   ```
   ./config.sh
   ```

5. On the Welcome screen, select **Extend an existing WebLogic domain**, and click **Next**.

6. On the Select a WebLogic Domain Directory screen, select the WebLogic Server domain directory (`ASERVER_HOME`), and click **Next**.

   In the reference topology, `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

7. On the Select Extension Source screen (Figure 14–1), make these selections:

- Select **Extend my domain automatically to support the following added products**.

- Select **Oracle WebCenter Enterprise Capture**.

  The following products are grayed out if they were selected when you created the domain (Section 8.3) or extended it for WebCenter Content (Section 10.2), Inbound Refinery (Section 11.2), Oracle SOA Suite components (Section 12.3), or Imaging (Section 13.3).

  * **Basic WebLogic Server Domain**

  * **Oracle SOA Suite**

  * **Oracle WebCenter Content: Imaging Viewer Cache**

  * **Oracle WebCenter Content: Imaging**

  * **Oracle Universal Content Management - Inbound Refinery**

  * **Oracle Universal Content Management - Content Server**

  * **Oracle Enterprise Manager Plugin for IBR**

  * **Oracle Enterprise Manager**

  * **Oracle WSM Policy Manager**

  * **Oracle JRF**

Figure 14–1   Select Extension Source Screen for Capture
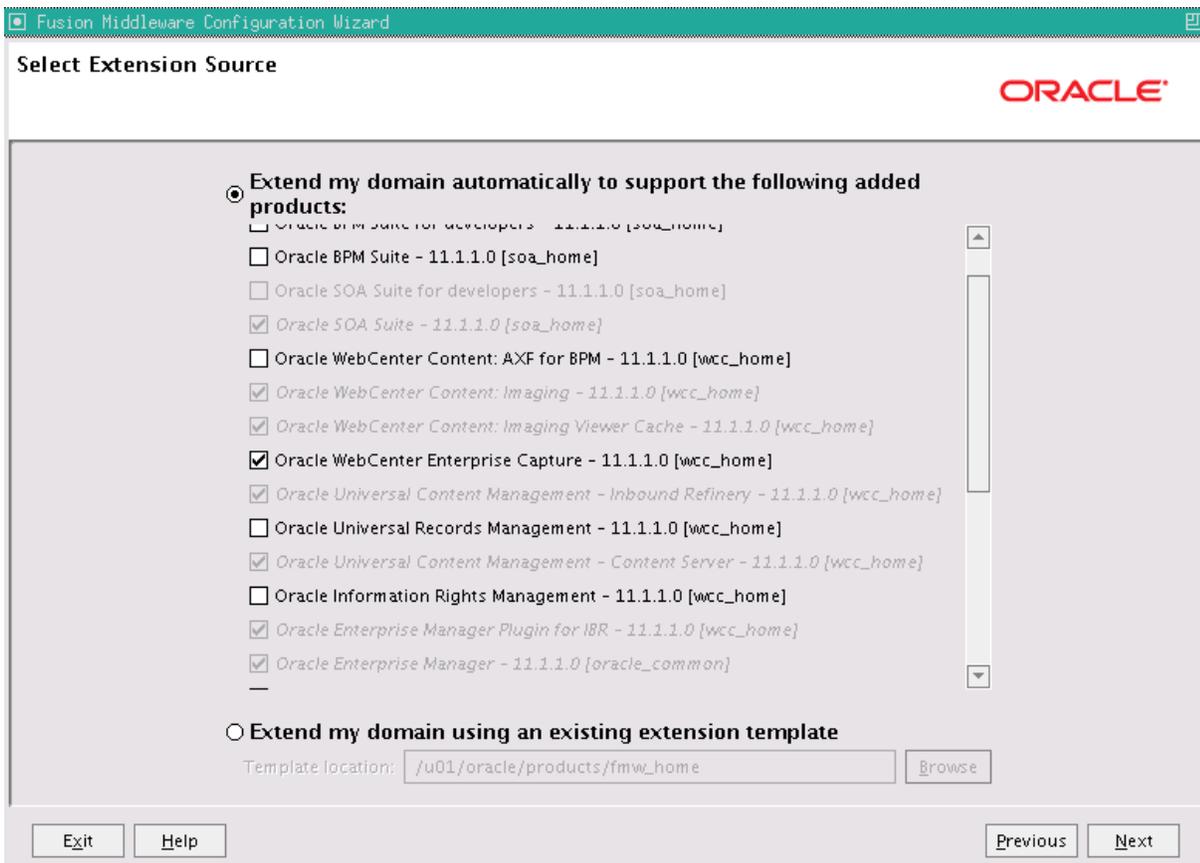
Click **Next**.

8. On the Configure JDBC Component Schema screen, which Figure 14–2 shows, perform the following steps:

   a. Select **Capture Schema** and **Capture MDS Schema**. 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.

Figure 14–2   Configure JDBC Component Schema Screen for Capture
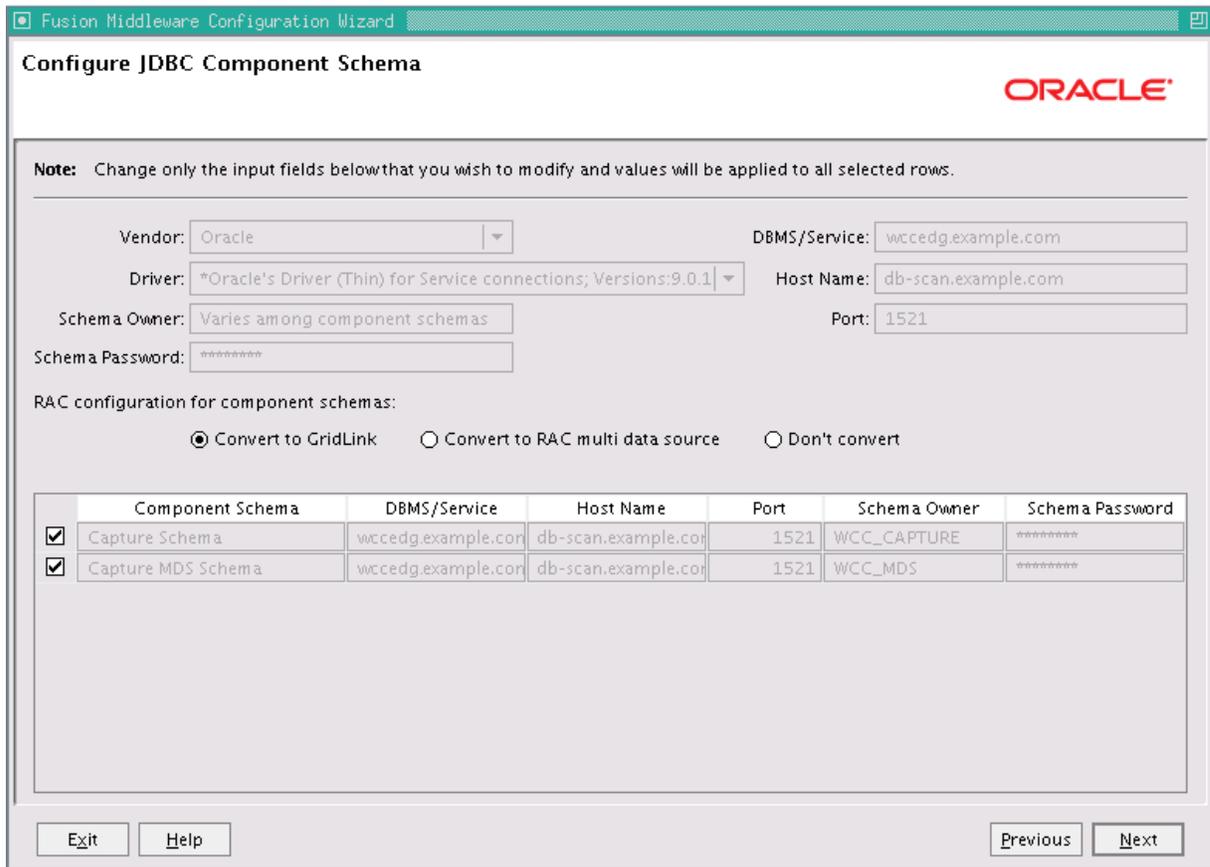
   c. Click **Next**.

9. On the Configure GridLink RAC Component Schema screen (Figure 14–3), perform the following steps:

   a. Select **Capture Schema** and **Capture MDS Schema**. Leave the other data sources as they are.

Figure 14–3 Configure GridLink RAC Component Schema Screen for Capture

b. Enter values for the following fields, specifying the connection information for the GridLink RAC database that was seeded through RCU:

– **Driver:** Select **Oracle's Driver (Thin) for GridLinkConnections; Versions: 11 and later**.

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

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

This book uses `WCC` 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>show parameter remote_listener;

NAME              TYPE       VALUE
-----             ------     -------
remote_listener   string     db-scan.example.com :1521
```

> **Note:** For Oracle Database 11*g*, use the virtual IP address and port of each database instance listener, as in these examples:
>
> `wccdbhost1-vip.example.com (port 1521)`
>
> `wccdbhost2-vip.example.com (1521)`

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

```
[orcl@WCCDBHOST1 ~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016
```

> **Note:** For Oracle Database 11*g*, use the host name and port of each database's ONS service, as in these examples:
>
> `wccdbhost1.example.com (port 6200)`
>
> `wccdbhost2.example.com (6200)`

c. Click **Next**.

> **Note:** Leave the **UCM Schema** information as is.

10. On the Test JDBC Component Schema screen, select the **CPT 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 14–4   Test JDBC Component Schema Screen for Capture
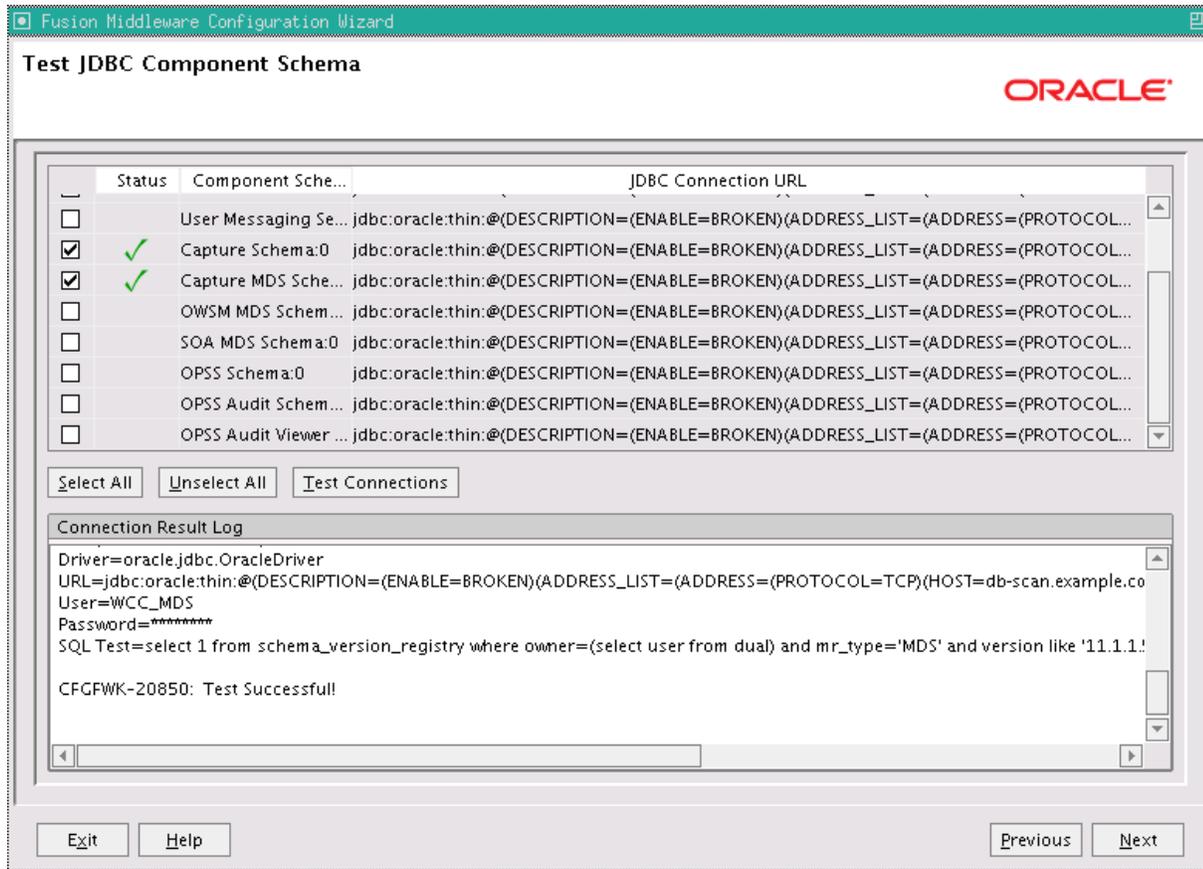
Click **Next** when the connection is successful.

11. On the Optional Configuration screen, select the following options:

    ■ **JMS Distributed Destination**

    ■ **Managed Servers, Clusters and Machines**

    ■ **Deployment and Services**

    Click **Next**.

12. On 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.

13. On the Configure Managed Servers screen, add the required Managed Servers.

    A server is created automatically. Rename this to WLS_CPT1 and add a new server called WLS_CPT2. Give these servers the attributes listed in Table 14–2. Do not modify the other servers that appear on this screen; leave them as they are.

Table 14–2   Managed Servers for Capture

Name	Listen Address	Listen Port	SSL Listen Port	SSL Enabled
WLS_CPT1	WCCHOST1VHN3	16400	n/a	No
WLS_CPT2	WCCHOST2VHN3	16400	n/a	No

Click **Next**.

14. On the Configure Clusters screen, click **Add** to add the clusters as shown in Table 14–3. Do not modify the other clusters that appear on this screen; leave them as they are.

Table 14–3   Cluster Configuration for Capture

Name	Cluster Messaging Mode	Multicast Address	Multicast Port	Cluster Address
CPT_Cluster	unicast	n/a	n/a	Leave empty.

Click **Next**.

15. On the Assign Servers to Clusters screen, add the following. Do not modify the other assignments that appear on this screen; leave them as they are.

- **CPT_Cluster:**
  - **WLS_CPT1**
  - **WLS_CPT2**

Click **Next**.

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

Table 14–4   Machines and Node Manager Listen Addresses

Name	Node Manager Listen Address
WCCHOST1	WCCHOST1
WCCHOST2	WCCHOST2
ADMINHOST	localhost

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

17. On the Assign Servers to Machines screen, assign servers to machines as follows:

- Assign **WLS_CPT1** to **WCCHOST1**.
- Assign **WLS_CPT2** to **WCCHOST2**.

Click **Next**.

18. On the Target Deployments to Clusters or Servers screen, make sure that targeting is done as follows:

- The **capture** deployment is targeted only to **CPT_Cluster**.
- **EM Application** is targeted only to **AdminServer**.

Click **Next**.

19. On the Target Services to Clusters or Servers screen, select all OPSS-related data sources to be deployed to **CPT_Cluster**, as Figure 14–5 shows:

- **opss-audit-viewDS**
- **opss-audit-DBDS**
- **opss-DBDS**

Figure 14–5   Target Services to the Capture Cluster
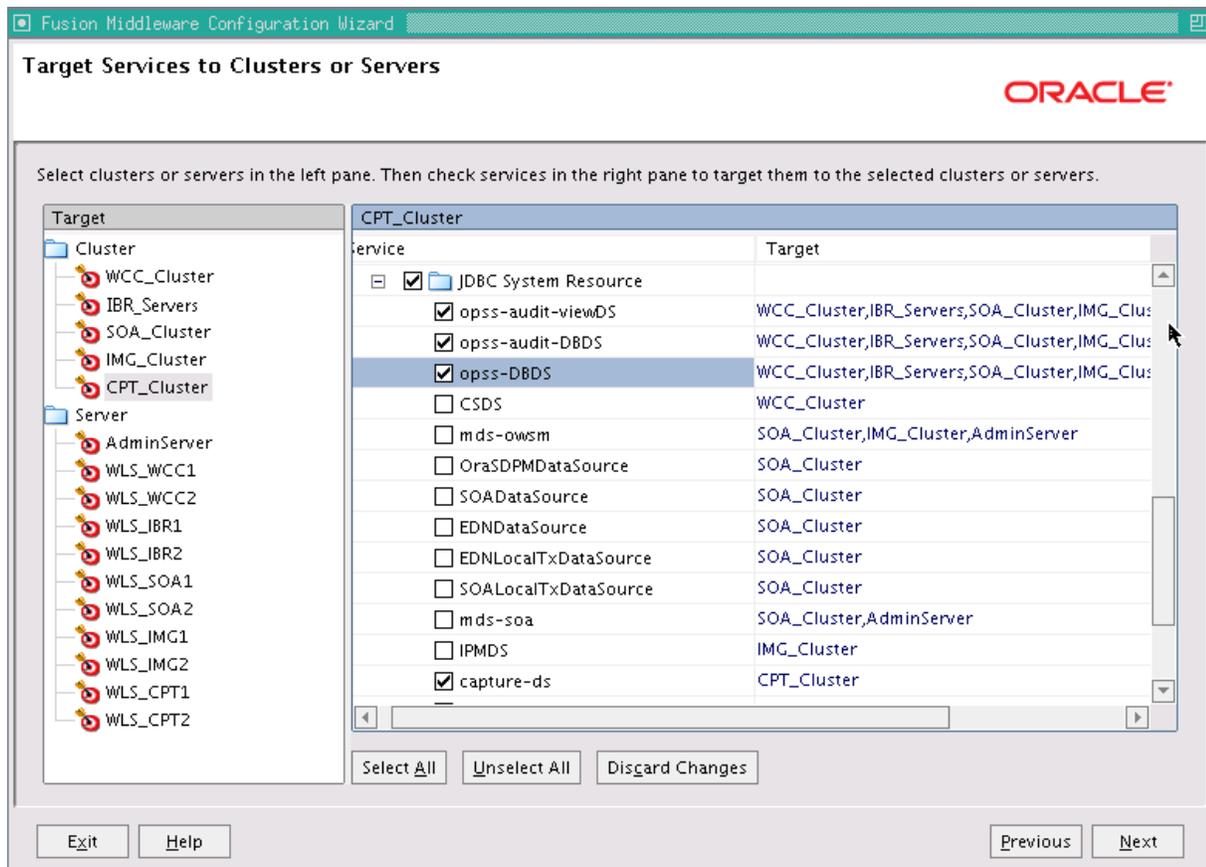
Click **Next**.

20. On the Configuration Summary screen, click **Extend**.

21. If a dialog box opens warning about conflicts in ports for the domain, click **OK**. This should be due to preexisting servers in the nodes and the warning can be ignored.

22. On the Creating Domain screen, click **Done**.

14.4 Restarting the Administration Server

You need to restart the Administration Server to make the domain extension changes take effect, using the Node Manager `nmKill` and `nmStart` commands through the Oracle WebLogic Scripting Tool (WLST), as described in Section 10.3, "Restarting the Administration Server." You can use the Administration Console instead of `nmKill` to stop the Administration Server. Log in to the Administration Console using the credentials for the `weblogic` user.

14.5 Completing Postconfiguration and Verification Tasks for Capture

The following sections describe how to do postconfiguration and verification tasks for Capture:

- Section 14.5.1, "Disabling Host Name Verification for the WLS_CPT Managed Servers"

- Section 14.5.2, "Propagating the Domain Configuration to WLS_CPT1 and WLS_CPT2"

- Section 14.5.3, "Completing the Initial Capture Configuration"

- Section 14.5.4, "Validating GridLink Data Sources for Capture"

- Section 14.5.5, "Configuring JMS Persistence Stores for Capture"

- Section 14.5.6, "Adding the Capture Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content"

14.5.1 Disabling Host Name Verification for the WLS_CPT 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 Capture. You must disable the host name verification for the WLS_CPT1 and WLS_CPT2 Managed Servers to avoid errors when managing the different WebLogic Server instances. For more information, see Section 8.4.5, "Disabling Host Name Verification."

You enable host name verification again once the enterprise deployment topology configuration is complete. For more information, see Section 16.3, "Enabling Host Name Verification Certificates for Node Manager."

14.5.2 Propagating the Domain Configuration to WLS_CPT1 and WLS_CPT2

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

To propagate the domain configuration to the Capture Managed Servers:

1. Create a copy of the Managed Server domain directory and the Managed Server applications directory.

2. Run the following `pack` command on WCCHOST1 to create a template pack:

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

   ```
   ./pack.sh -managed=true -domain=ASERVER_HOME -template=edgdomaintemplateCPT.jar
   -template_name=edgdomain_templateCPT
   ```

   In the reference topology, *ORACLE_COMMON_HOME* is the `/u01/oracle/products/fmw_home/oracle_common` directory, and *ASERVER_HOME* is the `/u01/oracle/config/domains/WCCDomain` directory.

3. Run the following `unpack` command on WCCHOST1 to propagate the template created in the preceding step to the WLS_CPT1 domain directory:

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

   ```
   ./unpack.sh -domain=MSERVER_HOME -template=edgdomaintemplateCPT.jar -app_
   dir=APPLICATION_HOME -overwrite_domain=true
   ```

In the reference topology, *MSERVER_HOME* is the
/u02/oracle/config/domains/WCCDomain directory, and *APPLICATION_HOME* is the
/u01/oracle/config/applications/WCCDomain directory.

> **Notes:**
>
> - Make sure to run unpack from the *ORACLE_COMMON_HOME*/common/bin/ directory, not from *WL_HOME*/common/bin/.
>
> - The *APPLICATION_HOME* directory gets backed up with this unpack command.
>
> - 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.

4. Run the following command on WCCHOST1 to copy the template pack created in step 1 to WCCHOST2:

```
scp edgdomaintemplateCPT.jar oracle@WCCHOST2:/u01/oracle/products/fmw_
home/oracle_common/bin
```

5. Run the following unpack command on WCCHOST2 to unpack the propagated template to the WLS_CPT2 Managed Server domain directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh –domain=/u02/oracle/config/domains/WCCDomain
-template=edgdomaintemplateCPT.jar –app_
dir=/u01/oracle/config/applications/WCCDomain –overwrite_domain=true
```

> **Notes:**
>
> - Make sure to run unpack from the *ORACLE_COMMON_HOME*/common/bin/ directory, not from *WL_HOME*/common/bin/.
>
> - The *APPLICATION_HOME* directory gets backed up with this unpack command.

6. Restart the Administration Server to make these changes take effect, stopping it with the nmKill command, or with the Administration Console, and then starting it with the nmStart command, as described in Section 10.3, "Restarting the Administration Server."

Before the restart, stop all Managed Servers in the domain through the Administration Console, and then start them after the restart. Log in to the Administration Console using the credentials for the weblogic user.

14.5.3 Completing the Initial Capture Configuration

To complete the initial configuration of Capture in a WebLogic Server domain, use the `weblogic` system administrator to do these tasks:

1. Start the Capture Managed Server.

2. Assign roles to Capture users in Fusion Middleware Control.

3. Modify system-level settings through MBeans.

14.5.3.1 About Completing the Initial Capture Configuration

The system administrator who performs the installation and initial configuration must have system administration permissions, including access to Oracle Enterprise Manager Fusion Middleware Control and Oracle WebLogic Server. Before anyone can use Oracle WebCenter Enterprise Capture, the system administrator needs to associate users from the LDAP identity store for the WebLogic Server domain with the Capture roles in Fusion Middleware Control.

To store groups and users, you can use the Oracle Internet Directory policy store. You can manage the policy store through Fusion Middleware Control.

The following Capture roles can be assigned to users:

- Capture Workspace Manager (`CaptureWorkspaceManager`)

- Capture Workspace Viewer (`CaptureWorkspaceViewer`)

- Capture User (`CaptureUser`)

The system administrator needs to assign the Workspace Manager both the `CaptureWorkspaceManager` and `CaptureUser` roles to provide access to the Workspace Console and the client. Only members of the `CaptureUser` role can use the Capture client. After an account has been granted the `CaptureWorkspaceManager` role, that account can sign in to the Workspace Console, create a workspace, and grant Capture access to other users who have been assigned Capture roles.

After starting the Capture Managed Server, the system administrator can modify system-level settings in Capture MBeans through Fusion Middleware Control or with Oracle WebLogic Scripting Tool (WLST) commands.

14.5.3.2 Starting the Capture Managed Servers

Start the Capture Managed Servers on WCCHOST1 and WCCHOST2.

To start the Capture Managed Servers:

1. Start the WLS_CPT1 Managed Server:

   a. Log in to the WebLogic Server Administration Console at `http://ADMINVHN:7001/console`.

   b. In the **Domain Structure** tree on the left, expand the **Environment** node, and then select **Servers**.

   c. On the Summary of Servers page, click the **Control** tab.

   d. Select **WLS_CPT1** from the **Servers** column of the table.

   e. Click **Start**.

2. Access `http://WCCHOST1VHN3:16400/dc-console` to verify the status of WLS_CPT1. The Oracle WebCenter Enterprise Capture Workspace Console login page opens. Enter your WebLogic Server administration user name and password to log in.

3. Start the WLS_CPT2 Managed Server:

a. Log in to the WebLogic Server Administration Console at `http://ADMINVHN:7001/console`.

b. In the **Domain Structure** tree on the left, expand the **Environment** node, and then select **Servers**.

c. On the Summary of Servers page, click the **Control** tab.

d. Select **WLS_CPT2** from the **Servers** column of the table.

e. Click **Start**.

4. Access `http://WCCHOST2VHN3:16400/dc-console` to verify the status of WLS_CPT2. The Oracle WebCenter Enterprise Capture Workspace Console login page opens. Enter your WebLogic Server administration user name and password to log in.

14.5.3.3 Assigning Roles to Capture Users

Before anyone uses Capture, the system administrator (`weblogic`) needs to assign users from the LDAP credential store to the Capture roles in the policy store. You can do this through the Application Roles page in Fusion Middleware Control.

To assign Capture roles to the Workspace Manager:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control.

2. On the left, expand **WebLogic Domain**.

3. Right-click the domain name, choose **Security**, and then choose **Application Roles**.

The Application Roles page opens.

Figure 14–6   Application Roles for Capture
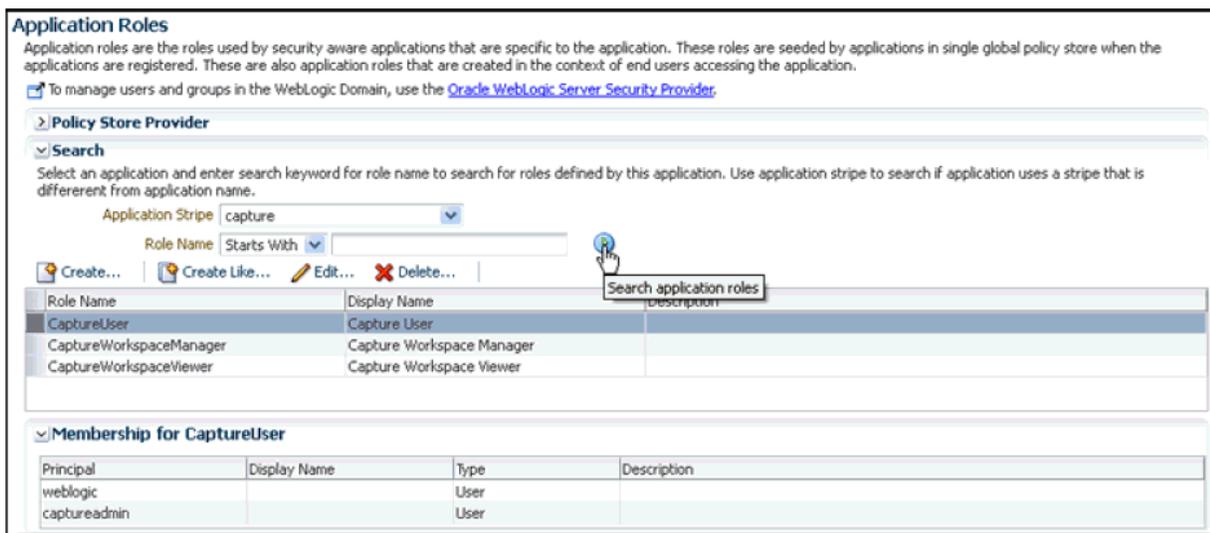
4. In the **Application Stripe** field, choose **capture** from the drop-down list, and then click the search icon.

The search populates the table with roles for the Capture User, Capture Workspace Manager, and Capture Viewer.

5. Edit the **CaptureWorkspaceManager** role.

6. Add a user to this role.

7. Edit the **CaptureUser** role.

8. Add the same user to this role, so that user has both the `CaptureWorkspaceManager` and `CaptureUser` roles.

For more information about how to assign roles to Capture users, see "Assigning Capture Roles in Oracle Enterprise Manager" in *Administering Oracle WebCenter Enterprise Capture*.

14.5.3.4 Modifying System-Level Settings Through MBeans

You can modify system-level configuration settings for Capture, including system properties and SMTP settings for email, through the System Configuration page in Fusion Middleware Control. The settings on this page configure the Capture MBeans for the domain, which you can also modify with WLST commands.

For information about how to modify system-level settings in Fusion Middleware control, see "Modifying System Configuration Settings" in *Administering Oracle WebCenter Enterprise Capture*.

The following WLST commands also enable you to access or modify system-level settings:

- `listCaptureConfig`

- `getCaptureConfig`

- `setCaptureConfig`

For more information about these commands, see "Oracle WebCenter Enterprise Capture Custom WLST Commands" in *Oracle Fusion Middleware WebLogic Scripting Tool Command Reference*.

14.5.4 Validating GridLink Data Sources for Capture

After the servers are started, verify that the GridLink data sources are correctly configured and that the ONS setup is correct. Perform this procedure for every GridLink data source created.

To verify the configuration of a GridLink data source for Capture:

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.

5. Click the **Testing** tab (Figure 14–7), select one of the servers, and click **Test Data Source**.

Figure 14–7 Testing a GridLink Data Source for Capture
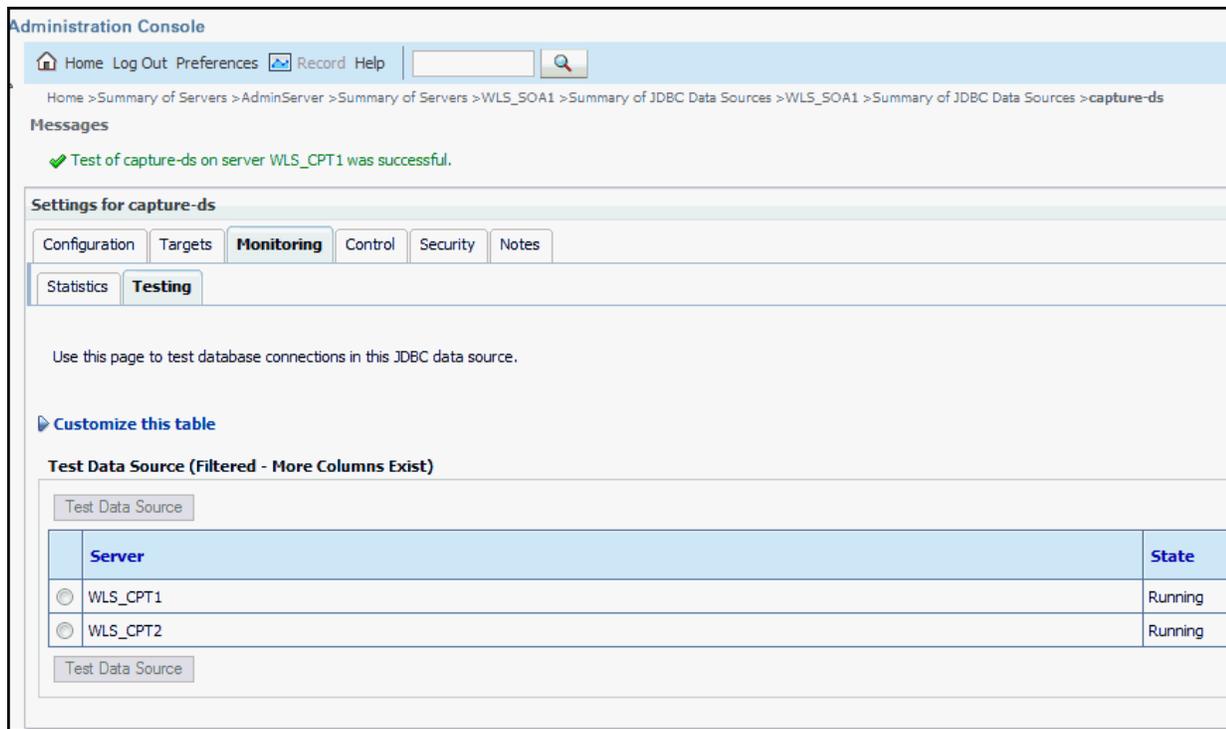
The test should be successful if the configuration is correct.

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 Capture:

1. In the **Domain Structure** tree on the Administration Console, expand **Services**, then click **Data Sources**.

2. Click the name of a GridLink data source.

3. Click the **Monitoring** tab.

4. Click the name of the server (`WLS_CPT1`).

5. Click the **ONS** tab and then the **Testing** tab (Figure 14–8).

6. Select a server, and click **Test ONS**.

Figure 14–8   Testing the ONS Configuration for Capture

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@WCCDBHOST1 ~]$ srvctl status scan_listener
SCAN Listener LISTENER_SCAN1 is enabled
SCAN listener LISTENER_SCAN1 is running on node WCCDBHOST1
SCAN Listener LISTENER_SCAN2 is enabled
SCAN listener LISTENER_SCAN2 is running on node WCCDBHOST2
SCAN Listener LISTENER_SCAN3 is enabled
SCAN listener LISTENER_SCAN3 is running on node WCCDBHOST2


[orcl@WCCDBHOST1 ~]$ srvctl config nodeapps -s
ONS exists: Local port 6100, remote port 6200, EM port 2016


[orcl@WCCDBHOST1 ~]$ srvctl status nodeapps | grep ONS
ONS is enabled
ONS daemon is running on node: WCCDBHOST1
ONS daemon is running on node: WCCDBHOST2
```

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

14.5.5 Configuring JMS Persistence Stores for Capture

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 Enterprise Capture are configured with no persistence store and use the WebLogic Server store (`/u02/oracle/config/domains/WCCDomain/servers/`*server_name*`/data/store/` default). You must change each Capture JMS server persistence store to use a shared base directory.

To configure JMS persistence stores for Capture:

1. Log in to the WebLogic Server Administration Console.

2. In the **Domain Structure** tree on the left, expand the **Services** node, and then click the **Persistence Stores** node.

3. On the Summary of Persistence Stores page, click **Lock & Edit**.

4. Click **New**, and then **Create File Store**.

5. Enter a **name** (for example, `CPTJMSServer1Store`, which allows you identify the service it is created for) and target WLS_CPT1. Enter a **directory** that is located in shared storage so that it is accessible from both WCCHOST1 and WCCHOST2 (`/u01/oracle/config/domains/WCCDomain/CPT_Cluster/jms`).

6. Click **OK** and activate the changes.

7. In the **Domain Structure** tree on the left, expand the **Services** node, and then click the **Messaging->JMS Servers** node.

8. On the Summary of JMS Servers page, click the **CaptureJmsServer1** JMS server (represented as a hyperlink) in the **Name** column of the table.

9. On the settings page for the JMS server, click **Lock & Edit**.

10. In the **Persistent Store** drop-down list, select **CPTJMSServer1Store**.

11. Click **Save and Activate**.

12. Repeat the steps and create `CPTJMSServer2Store` for **CaptureJMSServer2**.

14.5.6 Adding the Capture Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content

The settings of allowable hosts, configured for Oracle WebCenter Content Server in Section 13.5.11, "Adding the Imaging Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content," also applies to Capture with an addition of listeners for the Capture Managed Servers. If this is the first time Content Server allowable hosts are added (in the case of a non-Imaging Oracle WebCenter Content enterprise deployment setup), then the following configuration needs to be done from Content Server.

Add the host names of the WLS_CPT1 and WLS_CPT2 Managed Servers (WCCHOST1VHN3 and WCCHOST2VHN3, respectively) to the `SocketHostNameSecurityFilter` parameter list.

To add the Capture server listen addresses to allowed hosts in Oracle WebCenter Content:

1. Open the file `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs/config/config.cfg` in a text editor.

2. Remove or comment out the following line:

```
SocketHostAddressSecurityFilter=127.0.0.1|WCCHOST1-IP|WCCHOST2-IP|WEBHOST1-IP|WEBHOST2-IP
```

3. Add the following two lines to include the WLS_CPT1 and WLS_CPT2 listen addresses in the list of addresses that are allowed to connect to Oracle WebCenter Content:

```
SocketHostNameSecurityFilter=localhost|localhost.example.com|WEBHOST1|WEBHOST2|WCCHOST1|WCCHOST2|WCCHOST1VHN1|WCCHOST2VHN1|WCCHOST1VHN2|WCCHOST2VHN2|WCCHOST1VHN3|WCCHOST2VHN3|ucminternal.example.com|load-balancer-host-name
AlwaysReverseLookupForHost=Yes
```

> **Note:** The load balancer host name is the one that was used to configure the virtual servers in Section 3.3, "Load Balancers."

4. Save the modified `config.cfg` file, and restart the Oracle WebCenter Content servers, using the WebLogic Server Administration Console, for the changes to take effect.

14.6 Configuring Oracle HTTP Server for the Capture Cluster

To enable Oracle HTTP Server to route to CPT_Cluster, which contains the WLS_CPT1 and WLS_CPT2 Managed Servers, you must set the `WebLogicCluster` parameter to the list of nodes in the cluster.

This section includes the following topics:

- Section 14.6.1, "Configuring Oracle HTTP Server for the WLS_CPT Managed Servers"

- Section 14.6.2, "Setting the Front-End HTTP Host and Port"

- Section 14.6.3, "Validating Access Through the Load Balancer"

14.6.1 Configuring Oracle HTTP Server for the WLS_CPT Managed Servers

To configure Oracle HTTP Server for the WLS_CPT Managed Servers:

1. For each of the web servers on WEBHOST1 and WEBHOST2, add the following lines to the *ORACLE_INSTANCE*/config/OHS/ohs1/moduleconf/wcc_vh.conf and *ORACLE_INSTANCE*/config/OHS/ohs2/moduleconf/wcc_vh.conf files:

```
# DC-Console
<Location /dc-console>
    WebLogicCluster WCCHOST1VHN3:16400,WCCHOST2VHN3:16400
    SetHandler weblogic-handler
    WLCookieName JSESSIONID
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>
```

```
# DC-Client
<Location /dc-client>
    WebLogicCluster WCCHOST1VHN3:16400,WCCHOST2VHN3:16400
    SetHandler weblogic-handler
    WLCookieName JSESSIONID
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>
```

In the reference topology, *ORACLE_INSTANCE* is the `/u02/oracle/config/web1` or `/u02/oracle/config/web2` directory.

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

   `/u02/oracle/config/web`*N*`/bin/opmnctl restartproc ias-component=ohsX`

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

14.6.2 Setting the Front-End HTTP Host and Port

You must set the front-end HTTP host and port for the Capture cluster (CPT_Cluster).

To set the front-end HTTP host and port for the Capture cluster:

1. Log in to the WebLogic Server Administration Console.

2. Go to the Change Center section and click **Lock & Edit**.

3. Expand the **Environment** node in the **Domain Structure** tree on the left.

4. Click **Clusters**.

5. On the Summary of Clusters page, select **CPT_Cluster**.

6. Open the **HTTP** tab.

7. Set the following values:

   - **Frontend Host:** `wcc.example.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 front-end host directive in the cluster take effect.

14.6.3 Validating Access Through the Load Balancer

Verify URLs to ensure that appropriate routing and failover is working from the HTTP Server to CPT_Cluster.

To verify the URLs:

1. While WLS_CPT2 is running, stop WLS_CPT1 from the WebLogic Server Administration Console.

2. Access `http://wcc.example.com/dc-console` to verify that it is functioning properly. (You will not be able to retrieve reports or data because the Capture server is down.)

3. Start WLS_CPT1 from the WebLogic Server Administration Console.

4. Stop WLS_CPT2 from the WebLogic Server Administration Console.

5. Access `http://wcc.example.com/dc-console` to verify that it is functioning properly.

6. Start WLS_CPT2 from the WebLogic Server Administration Console.

14.7 Configuring Node Manager for the WLS_CPT Managed Servers

Oracle recommends using host name verification for 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. For more details, see Chapter 16, "Setting Up Node Manager for an Enterprise Deployment." The procedures in that chapter must be performed for the Oracle WebCenter Content deployment.

The procedures in Section 16.3, "Enabling Host Name Verification Certificates for Node Manager," must be performed for the hosts and Capture Managed Servers in the following table.

Host Name (*HOST*)	Virtual IP Address (*VIP*)	Server Name (*WLS_SERVER*)
WCCHOST1	WCCHOST1VHN3	WLS_CPT1
WCCHOST2	WCCHOST2VHN3	WLS_CPT2

For server migration of Capture Managed Servers, you need to associate these servers with the specified virtual host names. Check that these virtual host names are enabled by DNS or `/etc/hosts` resolution in your system and that they map to the appropriate virtual IP addresses. For more information, see Section 3.4, "IP Addresses and Virtual IP Addresses."

14.8 Configuring Server Migration for the WLS_CPT Managed Servers

Server migration is required for proper failover of the Oracle WebCenter Enterprise Capture components in the event of failure in any of the WCCHOST1 and WCCHOST2 nodes. For more details, see Chapter 17, "Configuring Server Migration for an Enterprise Deployment." For Capture, use the following values for the variables in that chapter:

- Server names:
  - *WLS_SERVER1*: WLS_CPT1
  - *WLS_SERVER2*: WLS_CPT2
- Host names:
  - *HOST1*: WCCHOST1
  - *HOST2*: WCCHOST2
- Cluster name:
  - *CLUSTER*: CPT_Cluster

14.9 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. For information on database backup, see the *Oracle Database Backup and Recovery Guide*.

To back up the installation at this point:

1. Back up Oracle Web Tier on WEBHOST1:

   a. Shut down the instance using `opmnctl`.

      ```
      /u02/oracle/config/webN/bin/opmnctl stopall
      ```

   b. Back up the Middleware home for Oracle Web Tier with the following command (as root):

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

   c. Back up the Oracle instance for Oracle Web Tier with the following command:

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

   d. Start the instance using `opmnctl`:

      ```
      cd /u02/oracle/config/webN/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 `/u01/oracle/config/domains/WCCDomain` directory. Run the following command on WCCHOST1 to create the backup:

   ```
   tar -cvpf edgdomainback.tar /u01/oracle/config/domains/WCCDomain
   ```

15

Installing and Configuring the WebCenter Content User Interface

This chapter describes how to install and configure an Oracle WebCenter Content Managed Server with the WebCenter Content user interface. This interface, for Oracle WebCenter Content Server, is based on the Oracle Application Development Framework (Oracle ADF).

This chapter includes the following sections:

- Section 15.1, "About Installing and Configuring the WebCenter Content User Interface"
- Section 15.2, "Preparing to Install and Configure the WebCenter Content User Interface"
- Section 15.3, "Installing an 11.1.1.6.0 Middleware Home with Oracle ADF 11.1.2"
- Section 15.4, "Installing the WebCenter Content User Interface Application"
- Section 15.5, "Deploying the WebCenter Content User Interface Application to a New Domain"
- Section 15.6, "Configuring the Administrator User"
- Section 15.7, "Accessing the WebCenter Content User Interface"
- Section 15.8, "Configuring Oracle HTTP Server with the WebCenter Content User Interface Cluster"
- Section 15.9, "Completing the Workflow Configuration"

15.1 About Installing and Configuring the WebCenter Content User Interface

You can configure Content Server with the WebCenter Content user interface in addition to the native 11*g* user interface, which Content Server uses by default. The WebCenter Content user interface resides in a separate domain from Content Server and runs on a different port, 16225 by default.

This separate domain requires its own Middleware home, which can reside on the same machine as the Middleware home for Content Server or on a separate machine. You could choose to have multiple instances of the WebCenter Content user interface server interact with the same Oracle WebCenter Content Server (previously known as Oracle UCM Content Server).

For a diagram of the WebCenter Content user interface domain topology, see Figure 1–2.

This chapter uses the following terminology:

- The first Middleware home contains Oracle WebCenter Content and is referred to as the Oracle WebCenter Content Middleware home (*MW_HOME* in directory paths).

- The first domain contains WebCenter Content and is referred to as the Oracle WebCenter Content domain (WCCDomain). This domain is associated with the Oracle WebCenter Content Middleware home.

- The second Middleware home contains the WebCenter Content user interface and is referred to as the WebCenter Content user interface Middleware home (*WCCUI_MW_HOME* in directory paths).

- The second domain contains the WebCenter Content user interface and is referred to as the WebCenter Content user interface domain (WCCUIDomain). This domain is associated with the WebCenter Content user interface Middleware home.

The WebCenter Content user interface domain requires its own Middleware home because changes are made to the Oracle ADF stack that are specifically required for the WebCenter Content user interface.

The two Middleware homes and domains can reside on the same host or on different hosts. The only additional requirement to run both domains on the same host is to use a different Administration Server port for each domain.

To install the WebCenter Content user interface and configure it for Content Server, you need to perform the tasks that the following sections describe.

15.2 Preparing to Install and Configure the WebCenter Content User Interface

Before you can install and configure the WebCenter Content User Interface, you need to install and configure Oracle WebCenter Content 11*g*R1 and, optionally, Inbound Refinery, as the previous chapters of this book describe.

All of the operations in this section pertain to the Oracle WebCenter Content Middleware home and, therefore, the Oracle WebCenter Content domain (WCCDomain).

Configure Oracle WebCenter Content Server as follows:

- Section 15.2.1, "Enabling WebCenter Content User Interface Components"

  This configuration is required for using the WebCenter Content user interface.

- Section 15.2.2, "Setting up the Remote Intradoc Client (RIDC)"

  This configuration is required for using the WebCenter Content user interface.

- Section 15.2.3, "Setting Additional Content Server Parameters"

  This configuration is optional, to set up additional configuration variables and the search engine for Content Server.

- Section 15.2.4, "Enabling Full-Text Searching"

  This configuration is optional, to set up Oracle Text Search.

- Section 15.2.5, "Generating Thumbnails and Web-Viewable Renditions"

  This configuration is optional, to enhance the WebCenter Content user interface experience.

- Section 15.2.6, "Configuring Extended Features in Content Server"

  This configuration is optional, to set up standard Content Server features.

- Section 15.8.1, "Configuring Oracle HTTP Server for the WLS_WCCUI Managed Servers"

  This configuration is required to set up Oracle HTTP Server.

- Section 15.8.2, "Validating Access Through the Load Balancer"

  This validation is required to test the earlier configuration.

15.2.1 Enabling WebCenter Content User Interface Components

Before you can use the WebCenter Content user interface, you must enable these Content Server components: AutoSuggestConfig, DynamicConverter, and FrameworkFolders. You can enable them through the Content Server Component Manager interface, as follows:

1. Log in to Content Server as a WebCenter Content administrator.

2. From the **Administration** tray or menu, choose **Admin Server**, then **Component Manager**.

3. On the Component Manager page, select all three components under **WebCenter Content UI Components**:

    - **AutoSuggestConfig**

    - **DynamicConverter**

    - **FrameworkFolders**

4. Click **Update**, and then click **OK** to confirm enabling the components.

5. Restart the WebCenter Content Managed Servers (WLS_WCC1 and WLS_WCC2), using the WebLogic Server Administration Console (stop and then start).

15.2.2 Setting up the Remote Intradoc Client (RIDC)

The WebCenter Content user interface uses the IDC socket protocol to communicate with Content Server. To enable this communication, you must set the `IntradocServerPort` and `SocketHostAddressSecurityFilter` values in the `ASERVER_HOME`/WCC_Cluster/cs/config/config.cfg configuration file for Content Server, in the Oracle WebCenter Content domain.

In the reference topology, `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

The following syntax shows how to set these values:

```
IntradocServerPort=port_number
SocketHostAddressSecurityFilter=IP addresses of permitted UI hosts separated by a
bar symbol (|)
AlwaysReverseLookupForHost=Yes
```

For example:

```
IntradocServerPort=4444
SocketHostNameSecurityFilter=localhost|localhost.example.com|WEBHOST1|WEBHOST2|
WCCHOST1|WCCHOST2||WCCUIHOST1|WCCUIHOST2|ucminternal.example.com|
load-balancer-host-name
AlwaysReverseLookupForHost=Yes
```

For more information about the `config.cfg` file, see "The config Directory" in *Oracle Fusion Middleware Developing with Oracle WebCenter Content*.

15.2.3 Setting Additional Content Server Parameters

For the WebCenter Content user interface, you can also set Content Server parameters for folders and searching.

To set additional Content Server parameters:

1. From the Content Server **Administration** menu or tray, choose **Admin Server** and then **General Configuration**.

2. Select the **Enable Accounts** checkbox.

3. In the Additional Configuration Variables area, add the following parameters, if not set already, to go in the `config.cfg` file:

   - `FoldersIndexParentFolderValues=true`

     This parameter enables you to search for content within folders, including subfolders.

   - `FldEnforceFolderFileNameUniqueness=true`

     This parameter prevents folders from having a child folder with the same name as a child document.

   - `FldEnforceCaseInsensitiveNameUniqueness=true`

     This parameter makes name-uniqueness checks for folder and file names case-insensitive. It also makes path resolution case-insensitive.

   - `SearchIndexerEngineName=OracleTextSearch` or `SearchIndexerEngineName=DATABASE.METADATA`

     This parameter enables OracleTextSearch full-text searching or database metadata searching, instead of the default database full-text searching.

4. Restart the WLS_WCC Managed Servers.

15.2.4 Enabling Full-Text Searching

For full-text searching, you need to rebuild the Content Server index using OracleTextSearch (`SearchIndexerEngineName=ORACLETEXTSEARCH` parameter).

To enable full-text searching in the WebCenter Content user interface:

1. Access Content Server with the native user interface:

   ```
   http://WCCHOST1:16200/cs
   ```

2. From the **Administration** menu or tray, choose **Admin Applets** and then **Repository Manager**.

3. Click the **Indexer** tab.

4. Under **Collection Rebuild Cycle**, click the **Start** button.

5. Deselect **Use Fast Rebuild**.

6. Click the **OK** button.

15.2.5 Generating Thumbnails and Web-Viewable Renditions

If you want to obtain thumbnail images and web-viewable renditions of files from the WebCenter Content user interface, you can configure Inbound Refinery to provide them. You can set up an Inbound Refinery provider for thumbnails and file conversions, such as PDF Export, through the native 11*g* user interface.

To configure thumbnails in Content Server:

1. Access Content Server with the native user interface:

   ```
   http://WCCHOST1:16200/cs
   ```

2. From the **Administration** menu or tray, choose **Configure Thumbnail Options**.

3. Select **Enable this server** to create the thumbnail images box.

4. Click the **Update** button.

For more information about generating thumbnails and web-viewable renditions, see "Configuring Inbound Refinery" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

15.2.6 Configuring Extended Features in Content Server

Some Content Server features are supported but not necessarily required by the WebCenter Content user interface. For example, Access Control Lists (ACLs) and Accounts are not configured out of the box. If these features are enabled on Content Server, however, the WebCenter Content user interface provides access to the additional functionality.

For information about enabling ACLs in Content Server, see "Managing Access Control List Security" in *Oracle Fusion Middleware Administering Oracle WebCenter Content*.

For information about enabling Accounts in Content Server, see "Managing Accounts" in *Oracle Fusion Middleware Administering Oracle WebCenter Content*.

These standard Content Server settings are not specific to the WebCenter Content user interface. For information about other extended features in Content Server, see *Oracle Fusion Middleware Administering Oracle WebCenter Content*.

15.3 Installing an 11.1.1.6.0 Middleware Home with Oracle ADF 11.1.2

Install Oracle Application Development Framework (Oracle ADF) 11*g*R1 (11.1.2) in an 11*g*R1 (11.1.1.6.0) Middleware home with Oracle WebLogic Server. This will include installing Oracle WebLogic Server 11gR1 (10.3.6 only) to create the Middleware home followed by installing Oracle ADF and then two Oracle ADF OPatch files. If your site is going to use Oracle WebCenter Content: Desktop with the WebCenter Content user interface, you also need to install a patch to support compatibility mode in Desktop 11.1.1.9.

> **Note:** You need to follow these steps exactly to enable the WebCenter Content user interface for Content Server 11.1.1.9. Even if you have Oracle Application Development Framework 11gR1 (11.1.2) available, you cannot use it for the WebCenter Content user interface 11.1.1.6.0 domain. Instead, you need to install Oracle ADF 11.1.1.6.0 and then upgrade it with patches to Oracle ADF 11.1.2.4.0, as the following instructions describe.

All the operations in this section pertain to the WebCenter Content user interface Middleware home and, therefore, to the WebCenter Content user interface domain. In the following commands, *WCCUI_MW_HOME* refers to the WebCenter Content user interface Middleware home, which includes the Oracle ADF installation.

For the WebCenter Content user interface domain, perform these steps on both hosts, WCCUIHOST1 and WCCUIHOST2:

1. Install Oracle WebLogic Server 11*g*R1 (10.3.6) to create a Middleware home. This will be the WebCenter Content user interface Middleware home (*WCCUI_MW_HOME*).

   In the reference topology, *WCCUI_MW_HOME* is the `/u01/oracle/products/fmw_home` directory.

2. Install Oracle Application Development Framework 11*g*R1 (11.1.1.6.0) in *WCCUI_MW_HOME*):

   a. Obtain the Oracle Application Development Framework 11*g*R1 (11.1.1.6.0) media, as described in "Software Downloads for Oracle WebCenter Content Installation and Configuration" in *Oracle Fusion Middleware Installing and Configuring Oracle WebCenter Content*.

   b. Unzip the ZIP file containing Oracle ADF to a temporary location, *media_loc*.

   c. Run the installer, using the following command:

   `media_loc/Disk1/runInstaller -jreLoc WCCUI_MW_HOME/jrockit_160_24_D1.1.2-4`

3. Obtain the Oracle Application Development Framework 11*g*R1 (11.1.2.4.0) OPatch 16546129 (`p16546129_111160_Generic.zip`) from My Oracle Support (formerly Oracle*MetaLink*) at `https://support.oracle.com`.

4. Unzip the patch ZIP file into a temporary folder, *temp_location*, and then run the following command:

   `WCCUI_MW_HOME/oracle_common/OPatch/opatch apply -jre WCCUI_JAVA_HOME/jre -oh WCCUI_MW_HOME/oracle_common/ temp_location/16546129`

   In the reference topology, *WCCUI_JAVA_HOME* is the `/u01/oracle/products/fmw_home/jrockit_160_24_D1.1.2-4` directory (the location of the JDK).

5. Obtain the Oracle Application Development Framework 11*g*R1 (11.1.2) OPatch 16546157 (`p16546157_111160_generic.zip`) from `https://support.oracle.com`.

6. Unzip the patch ZIP file into a temporary folder, *temp_location*, and run the following command:

   `WCCUI_MW_HOME/oracle_common/OPatch/opatch apply -jre WCCUI_JAVA_HOME/jre -oh WCCUI_MW_HOME/oracle_common/ temp_location/16546157`

7. (Optional) For MDS customizing of the WebCenter Content user interface, obtain patch number 16020846, version 11.1.2.4.0 (`p16020846_111240_Generic.zip`), from `https://support.oracle.com`.

8. (Optional) Unzip the patch ZIP file into a temporary folder, *temp_location*, and run the following command:

   `WCCUI_MW_HOME/oracle_common/OPatch/opatch apply -jre WCCUI_JAVA_HOME/jre -oh WCCUI_MW_HOME/oracle_common/ temp_location/16020846`

9. (Optional) For Internet Explorer 11 renditions, obtain patch number 19469801, version 11.1.2.4.0 (`p19469801_111240_Generic.zip`), from `https://support.oracle.com`.

10. (Optional) Unzip the patch ZIP file into a temporary folder, *temp_location*, and run the following command:

    WCCUI_MW_HOME/oracle_common/OPatch/opatch apply -jre *WCCUI_JAVA_HOME*/jre -oh *WCCUI_MW_HOME*/oracle_common/ *temp_location/19469801*

11. (Optional) For Oracle ADF Help, obtain patch number 18102108, version 11.1.2.4.0 (p18102108_111240_Generic.zip), from https://support.oracle.com.

12. (Optional) Unzip the patch ZIP file into a temporary folder, *temp_location*, and run the following command:

    WCCUI_MW_HOME/oracle_common/OPatch/opatch apply -jre *WCCUI_JAVA_HOME*/jre -oh *WCCUI_MW_HOME*/oracle_common/ *temp_location/18102108*

15.4 Installing the WebCenter Content User Interface Application

You need to install the WebCenter Content User Interface application on WCCHOST1 and on WCCHOST2. The WebCenter Content user interface artifacts are in a ZIP file called WccADFUI.zip, which you can obtain from the WebCenter Content Oracle home in the Oracle WebCenter Content (first) Middleware home. The file location is *WCC_ORACLE_HOME*/ucm/Distribution/WccADFUI/WccADFUI.zip.

In the reference topology, *WCC_ORACLE_HOME* is the /u01/oracle/products/fmw_home/wcc_home directory on WCCHOST1 or WCCHOST2.

The WccADFUI.zip file includes these WebCenter Content user interface artifacts:

- The application EAR file, WccAdf.ear
- The domain extension configuration template
- Custom Oracle Weblogic Scripting Tool (WLST) commands for managing the connections to Oracle WebCenter Content Server
- Support scripts for deployment and management of the application

To install the WebCenter Content user interface application, perform these steps on WCCHOST1 and on WCCHOST2:

1. Create the directory *WCCUI_MW_HOME*/oracle_common/webcenter/wccadf in the WebCenter Content user interface (second) Middleware home.

   In the reference topology, *WCCUI_MW_HOME* is the /u01/oracle/products/fmw_home directory on WCCUIHOST1 or WCCUIHOST2.

2. Copy the *WCC_ORACLE_HOME*/ucm/Distribution/WccADFUI/WccADFUI.zip file to the *WCCUI_MW_HOME*/oracle_common/webcenter/wccadf directory.

3. Expand the ZIP file in the *WCCUI_MW_HOME*/oracle_common/webcenter/wccadf directory.

15.5 Deploying the WebCenter Content User Interface Application to a New Domain

You need to deploy the WebCenter Content user interface application to a new WebLogic Server domain on WCCUIHOST1 and copy the domain configuration to WCCUIHOST2 before you can use the application with the Content Server application in the Oracle WebCenter Content domain. After configuration of both domains is complete, you can use either the WebCenter Content user interface or the native 11*g* user interface with Content Server.

> **Note:** All of the operations in this section pertain to the WebCenter Content user interface Middleware home and, therefore, to the WebCenter Content user interface domain.

To deploy the WebCenter Content user interface application to a new domain, you need to perform these tasks:

1. Registering the MDS Repository

2. Running the Configuration Wizard on WCCUIHOST1 to Create a Domain

3. Performing Postconfiguration and Verification Tasks for the Domain

4. Registering the WCCUI Managed Servers with MDS and Creating a Metadata Partition

5. Propagating the Domain Configuration to WLS_WCCUI1 and WLS_WCCUI2

6. Associating the WebCenter Content User Interface with Content Server

15.5.1 Registering the MDS Repository

To register the Oracle Metadata Services (MDS) repository in the WebCenter Content user interface application, perform these steps on WCCHOST1:

1. Run WLST from the WebCenter Content user interface Middleware home:

   ```
   WCCUI_MW_HOME/oracle_common/common/bin/wlst.sh
   ```

   In the reference topology, *WCCUI_MW_HOME* is the `/u01/oracle/products/fmw_home` directory.

2. Run the following commands in offline mode:

   ```
   wls:/offline> archive = getMDSArchiveConfig('WCCADF_EAR_LOCATION')

   wls:/offline> archive.setAppMetadataRepository(repository='mds-mds_repo_name',
   partition='partition_name', type='DB', jndi='jdbc/mds/mds_repo_name')

   wls:/offline> archive.save()
   ```

   In the `getMDSArchiveConfig` command, *WCCADF_EAR_LOCATION* is the directory where the `WccADFUI.zip` file was expanded, *WCCUI_MW_HOME*/`oracle_common/webcenter/wccadf` in the reference topology.

   In the `archive.setAppMetadataRepository` command, *mds_repo_name* is the name of the repository, and *partition_name* is a name for the partition to be created.

For example:

```
archive =
getMDSArchiveConfig('/u01/oracle/products/fmwhome/ADFMW/oracle_
common/webcenter/wccadf/WccAdf.ear')
archive.setAppMetadataRepository(repository='mds-WCCUIMDSREPO', partition='MDS_
PARTITION', type='DB', jndi='jdbc/mds/WCCUIMDSREPO')
archive.save()
```

15.5.2 Running the Configuration Wizard on WCCUIHOST1 to Create a Domain

To run the Fusion Middleware Configuration Wizard on WCCUIHOST1 to create a domain:

1. In the WebCenter Content user interface Middleware home, copy the WebCenter Content user interface domain template, `oracle.ucm.cs_adf_template_11.1.1.jar`, from the `WCCUI_MW_HOME`/oracle_common/webcenter/wccadf directory to the following directory:

   `WCCUI_MW_HOME`/oracle_common/common/templates/applications

   In the reference topology, `WCCUI_MW_HOME` is the `/u01/oracle/products/fmw_home` directory.

2. Run the Configuration Wizard in the WebCenter Content user interface Middleware home:

   `WCCUI_MW_HOME`/oracle_common/common/bin/config.sh

3. On the Welcome screen, select **Create a new WebLogic Domain**, and click **Next**.

4. The Select Domain Source screen opens (Figure 15–1).

Figure 15–1   Select Domain Source for the WebCenter Content User Interface
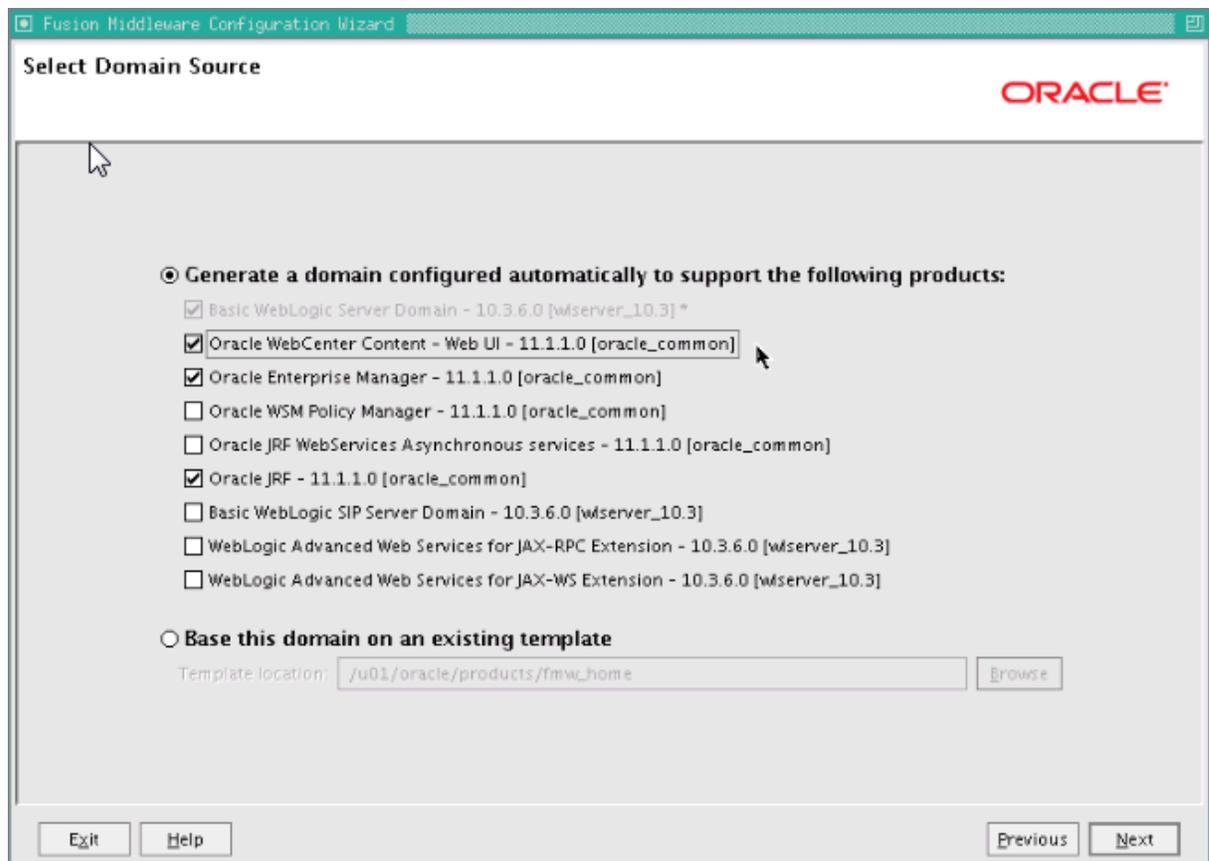
On the Select Domain Source screen, perform the following steps:

a. Select **Generate a domain configured automatically to support the following products**.

b. Select the following products:

– **Basic WebLogic Server Domain** (this should be selected automatically)

– **Oracle WebCenter Content - Web UI**

– **Oracle Enterprise Manager** (selected automatically)

– **Oracle JRF** (selected automatically)

c. Click **Next**.

5. On the Specify Domain Name and Location screen, enter the name of the new domain, such as WCCUIDomain, and the domain and applications directories:

■ **Domain name:** WCCUIDomain

■ **Domain location:** /u01/oracle/config/domains

■ **Application location:** /u01/oracle/config/applications

The Configuration Wizard adds a subdirectory with the domain name to the domain location, to make the *WCCUI_ASERVER_HOME* directory, and to the application location, to make the *WCCUI_APPLICATION_HOME* directory.

Make sure that these directories match the directory and shared-storage mount points recommended in Chapter 4, "Preparing the File System for an Enterprise Deployment." The Managed Server domain directory for WebCenter Content user interface should be under the local volume for each server.

Click **Next**.

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

Click **Next**.

7. On the Configure Server Start Mode and JDK screen, perform the following steps:

■ For WebLogic Domain Startup Mode, select **Production Mode**.

■ For JDK Selection, select **JROCKIT SDK1.6.0_***version*.

Note: The examples documented in this guide use Oracle JRockit. Any certified version of Java can be used for this procedure and is fully supported unless otherwise noted.

Click **Next**.

8. On the Select Optional Configuration screen, select the following:

■ **Administration Server**

■ **Managed Servers, Clusters and Machines**

■ **Deployments and Services**

Click **Next**.

9. On the Configure the Administration Server screen, enter the following values:

   ■ **Name:** `AdminServer`

   ■ **Listen address:** `WCCUIADMINVHN`.

   ■ **Listen port:** `7001`

   The default port number for the Administration Server is `7001`. If you are configuring the WebCenter Content user interface domain on the same machine as the Oracle WebCenter Content domain, use a different port number.

   ■ **SSL listen port:** `N/A`

   ■ **SSL enabled:** Leave this checkbox unselected.

   Click **Next**.

10. On the Configure Managed Servers screen, configure WLS_WCCUI1 and WLS_WCCUI2 as Figure 15–2 shows.

Figure 15–2 Configuration Screen for WLS_WCCUI Managed Servers
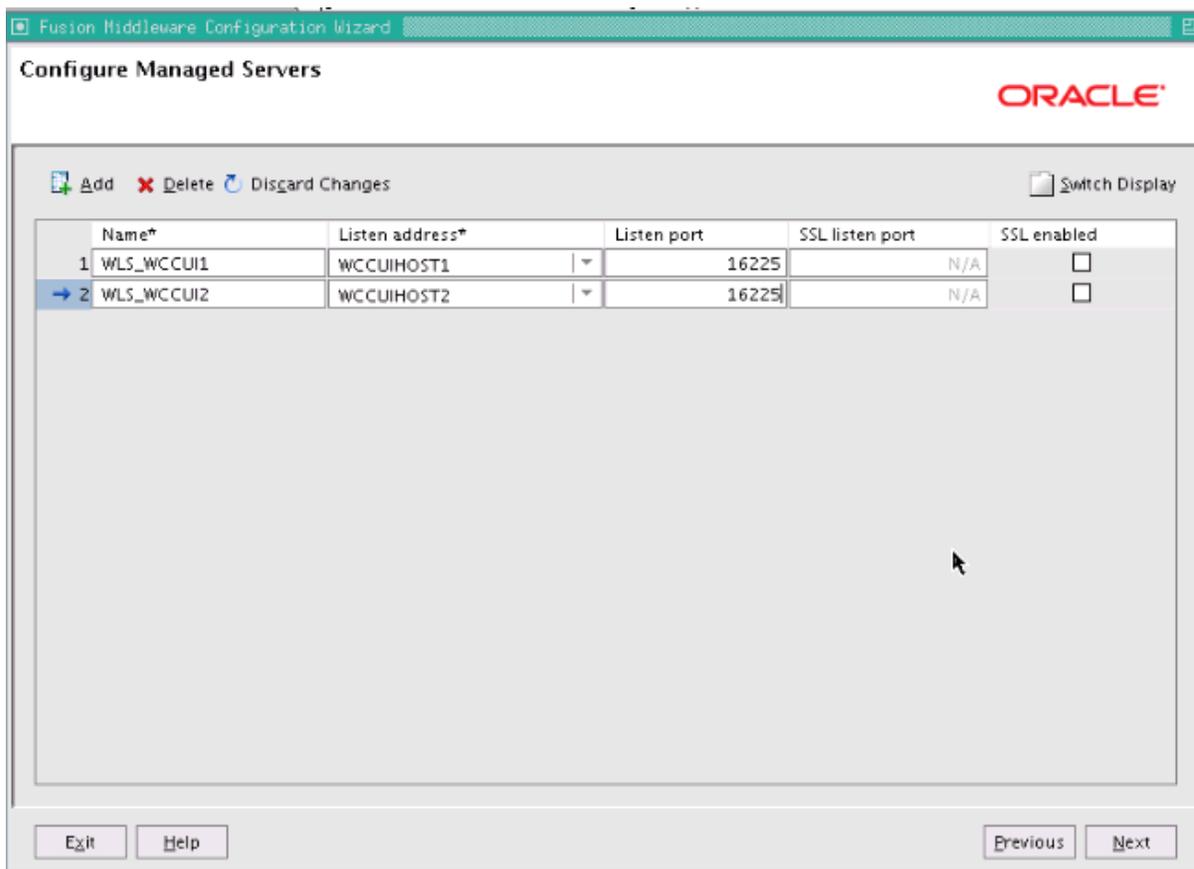
   Click **Next**.

11. On the Configure Clusters screen, configure WCCUI_Cluster as Figure 15–3 shows.

Figure 15–3   Configure Clusters Screen for WCCUI_Cluster
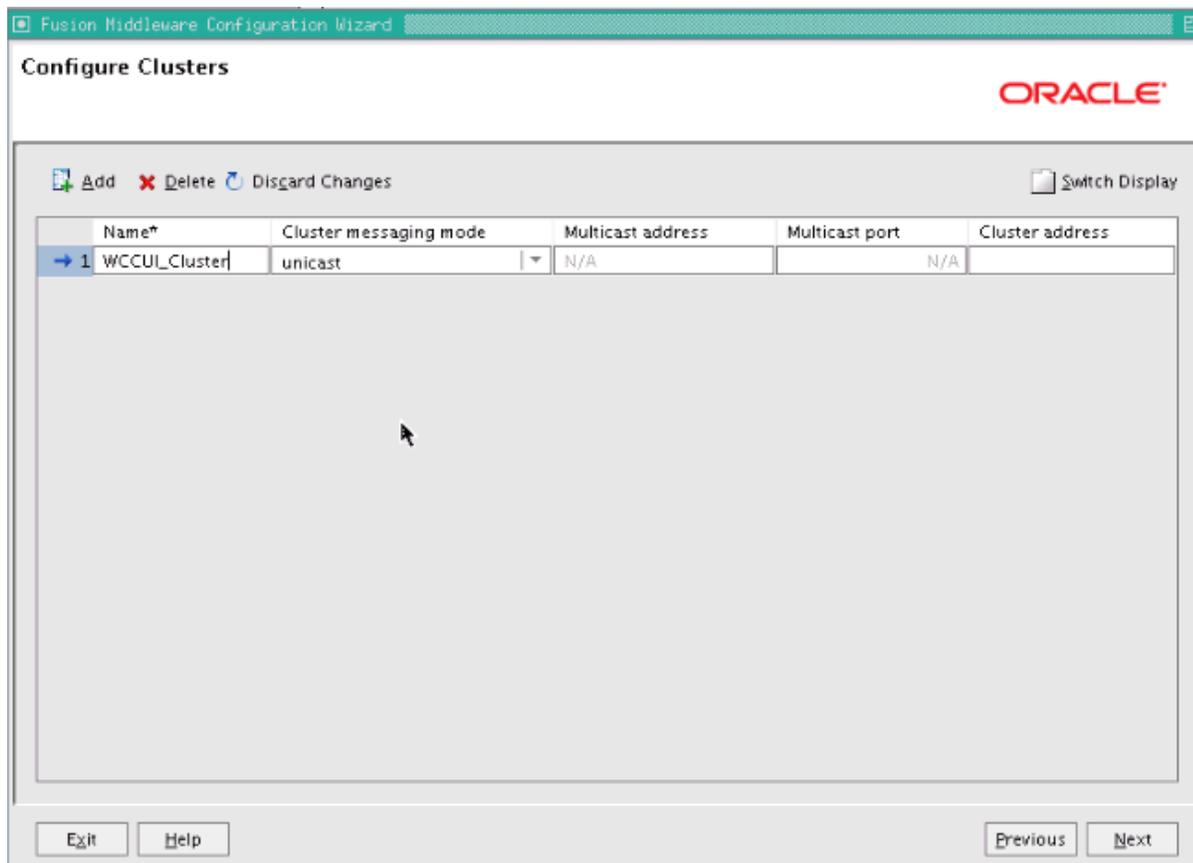
Click **Next**.

12. On the Assign Servers to Clusters screen, assign each Managed Server to WCCUI_Cluster, as Figure 15–4 shows.

Figure 15–4   Assign Managed Servers to WCCUI_Cluster
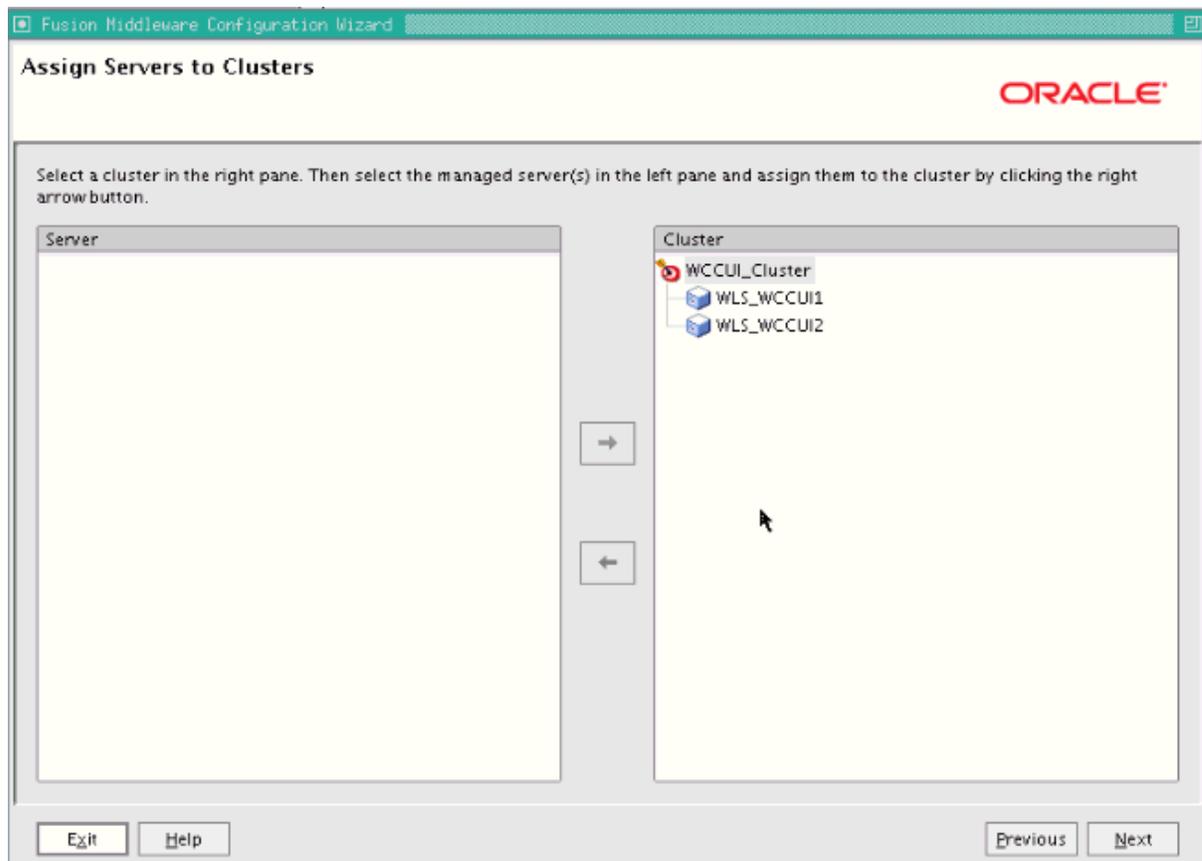
Click **Next**.

13. On the Configure Machines screen, open the **Unix Machine** tab and then click **Add** to add the **WCCUIADMINHOST**, **WCCUIHOST1**, and **WCCUIHOST2** machines, configured as Figure 15–5 shows.

Figure 15–5   Configure Machines Screen for WCCUI Hosts
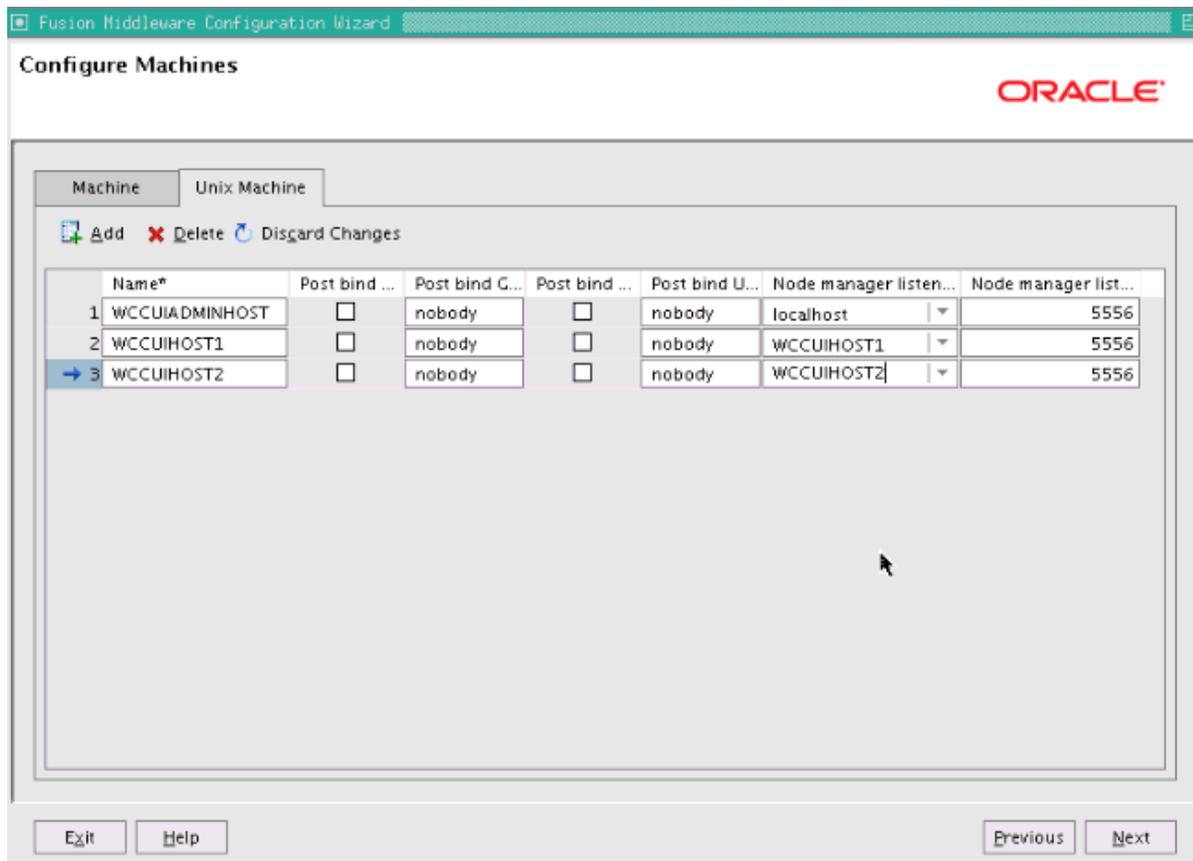
The machine names do not need to be a valid host names or listen addresses. Each name is a unique identifier of a Node Manager location.

> **Note:** The virtual host machine for the Administration Server must point to `localhost` because `localhost` is the relative internal address for whatever machine is active. The Node Manager instance associated with the Administration Server changes when the Administration Server fails over because the Administration Server uses the `localhost` attribute in conjunction with the first host and then again, after failover, in conjunction with the second host.

Click **Next**.

14. On the Assign Servers to Machines screen, assign the Administration Server and Managed Servers to a machines as Figure 15–6 shows.

Figure 15–6   Assign WCCUI Servers to Machines
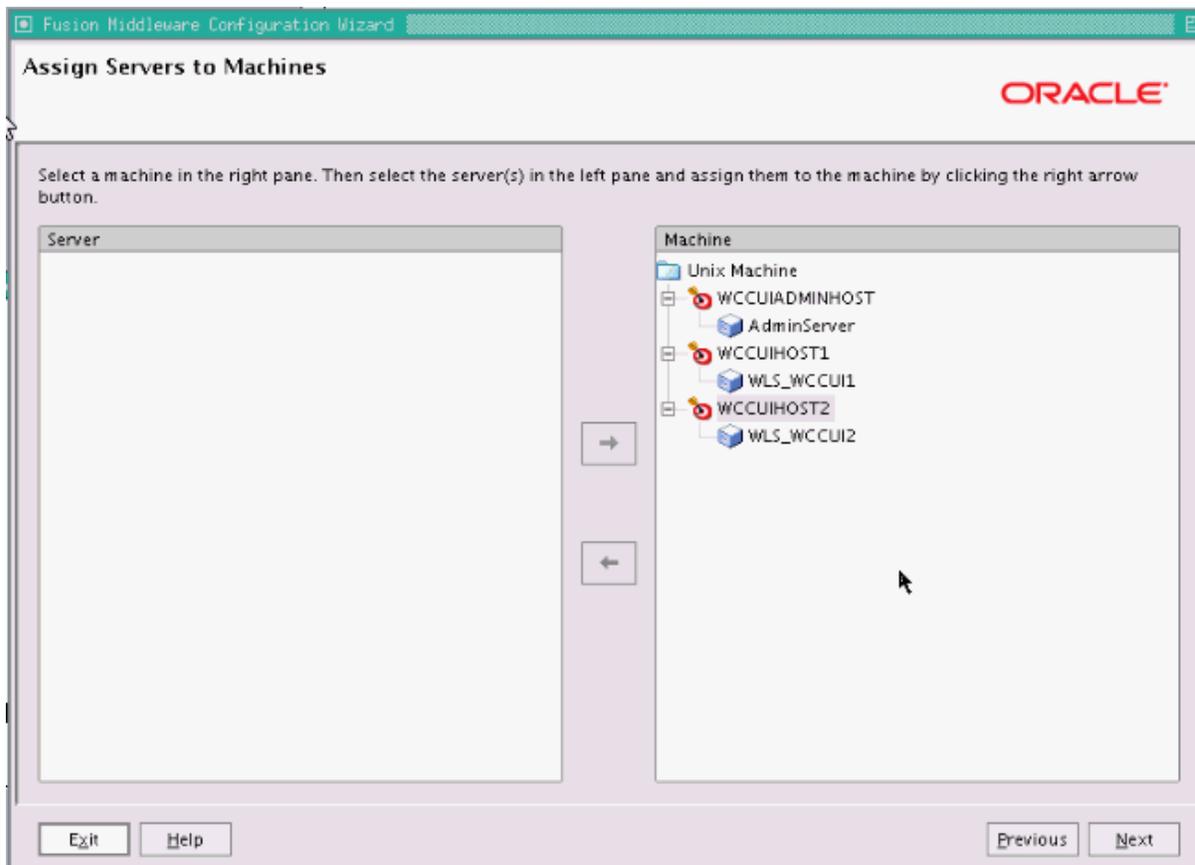
Click **Next**.

15. On the Target Deployments to Clusters or Servers screen, click **Next**.

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

17. On the Configuration Summary screen, click **Create**.

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

This procedure will create a new domain and a Managed Server for the WebCenter Content user interface application. You will not need any data sources to be set up for this application.

15.5.3 Performing Postconfiguration and Verification Tasks for the Domain

After configuring the domain with the Configuration Wizard, follow these instructions for postconfiguration and verification.

The section includes the following topics:

- Section 15.5.3.1, "Upgrading the Oracle ADF Shared Libraries to Sherman Update 2"

- Section 15.5.3.2, "Creating boot.properties for the Administration Server on WCCUIHOST1"

- Section 15.5.3.3, "Starting Node Manager on WCCUIHOST1"

- Section 15.5.3.4, "Starting the Administration Server on WCCUIHOST1"

- Section 15.5.3.5, "Validating the Administration Server Configuration"

- Section 15.5.3.6, "Disabling Host Name Verification"

- Section 15.5.3.7, "Copying the Domain Registry File to the Middleware Home on WCCUIHOST2"

15.5.3.1 Upgrading the Oracle ADF Shared Libraries to Sherman Update 2

To upgrade the Oracle ADF shared libraries in the WebCenter Content user interface domain to Sherman Update 2:

a. Run WLST from the *WCCUI_ORACLE_COMMON_HOME*/common/bin directory, as shown in the following example:

```
cd /u01/oracle/products/fmw_home/oracle_common/common/bin

./wlst.sh


Initializing WebLogic Scripting Tool (WLST) ...

Welcome to WebLogic Server Administration Scripting Shell

Type help() for help on available commands

wls:/offline>
```

In the reference topology, *WCCUI_ORACLE_COMMON_HOME* is the /u01/oracle/products/fmw_home/oracle_common directory.

b. Run the following command in offline mode:

```
wls:/offline> upgradeADF('WCCUI_ASERVER_HOME');
```

For example:

```
wls:/offline> upgradeADF('/u01/oracle/config/domains/WCCUIDomain')
Target Library "jsf#2.0@1.0.0.0_2-0-2" to JRF "WCCUI_Cluster"
Target Library "jsf#2.0@1.0.0.0_2-0-2" to JRF "AdminServer"
```

In the reference topology, *WCCUI_ASERVER_HOME* is the /u01/oracle/config/domains/WCCUIDomain directory.

15.5.3.2 Creating boot.properties for the Administration Server on WCCUIHOST1

Create a `boot.properties` file for the Administration Server on WCCUIHOST1. This file enables the Administration Server to start without prompting you for the administrator user name and password.

To create a `boot.properties` file for the Administration Server on WCCUIHOST1:

1. Create the following directory structure on WCCUIHOST1:

   ```
   mkdir -p WCCUI_ASERVER_HOME/servers/AdminServer/security
   ```

   In the reference topology, *WCCUI_ASERVER_HOME* is the `/u01/oracle/config/domains/WCCUIDomain` directory.

2. In a text editor, create a file called `boot.properties` in the directory created in the previous step, and enter the following lines into the file:

   ```
   username=admin_user
   password=admin_password
   ```

   The values of *admin_user* and *admin_password*, are the user name and password of the WebLogic Server domain administrator.

   > **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 15.5.3.4, "Starting the Administration Server on WCCUIHOST1." 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.

15.5.3.3 Starting Node Manager on WCCUIHOST1

To start Node Manager on WCCUIHOST1, set the `StartScriptEnabled` property to `true`, and then start Node Manager using `startNodeManager.sh`.

To start Node Manager on WCCUIHOST1:

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

   ```
   cd WCCUI_ORACLE_COMMON_HOME/common/bin

   ./setNMProps.sh
   ```

   In the reference topology, *WCCUI_ORACLE_COMMON_HOME* is the `/u01/oracle/products/fmw_home/oracle_common` directory.

2. Start Node Manager:

   ```
   cd WCCUI_WL_HOME/server/bin

   export JAVA_OPTIONS=-DDomainRegistrationEnabled=true

   nohup ./startNodeManager.sh > nm.out&
   ```

In the reference topology, `WCCUI_WL_HOME` is the `/u01/oracle/products/fmw_home/wlserver_10.3` directory.

> **Note:** It is important to set the `-DDomainRegistrationEnabled=true` parameter whenever Node Manager is started, to manage the Administration Server. If there is no Administration Server on the machine and the machine is not an Administration Server failover node, then you can start Node Manager with the following script (without the `export` command).
>
> ```
> nohup ./startNodeManager.sh > nm.out&
> ```

15.5.3.4 Starting the Administration Server on WCCUIHOST1

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 Fusion Middleware Configuration Wizard set for Node Manager. You must therefore use the start script for the Administration Server for the first start. In the following procedure, steps 1 through 4 are required for the first start; all subsequent starts require only step 4.

To start the Administration Server on WCCUIHOST1:

1. On WCCUIHOST1, start the Administration Server using the start script in the domain directory:

   ```
   cd WCCUI_ASERVER_HOME/bin

   ./startWebLogic.sh
   ```

   In the reference topology, `WCCUI_ASERVER_HOME` is the `/u01/oracle/config/domains/WCCUIDomain` directory.

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

   a. Open a web browser and go to `http://WCCUIADMINVHN:7001/console`.

   b. Log in as `weblogic`.

   c. Click **Lock & Edit**.

   d. Click *domain_name*, then **Security**, and then **General**, and 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 WebLogic Server Administration Server by issuing the command `stopWebLogic.sh` located in the `WCCUI_ASERVER_HOME/bin` directory.

   Alternatively, you can 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 WCCUI_ORACLE_COMMON_HOME/common/bin

   ./wlst.sh
   ```

In the reference topology, *WCCUI_ORACLE_COMMON_HOME* is the `/u01/oracle/products/fmw_home/oracle_common` directory.

Once in the WLST shell, execute the following commands (make sure Node Manager is up and running):

```
wls:/offline>nmConnect("node_admin_user","node_admin_password",
"WCCUIHOST1","5556", "domain_name","WCCUI_ASERVER_HOME")

wls:/nm/domain_name> nmStart("AdminServer")
```

Notes:

- WCCUIHOST1 is the address of the node where the domain was created, not the listen address of the Administration Server.

- The values of *node_admin_user* and *node_admin_password* are the Node Manager credentials that were updated in Step 2e. Independent from the server administrator ID and password, the Node Manager administrator user name and password are used only to authenticate connections between Node Manager and clients. These credentials are stored in the *WCCUI_ASERVER_HOME*/config/nodemanager/nm_password.properties file.

15.5.3.5 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 Administration Server 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://WCCUIADMINVHN:7001/console`.

2. Log in as the administrator.

3. Check that you can access Fusion Middleware Control at `http://WCCUIADMINVHN:7001/em`.

4. Log in to Fusion Middleware Control with the user name and password you specified in Section 15.5.3.2, "Creating boot.properties for the Administration Server on WCCUIHOST1."

The Administration Server should be up and running.

15.5.3.6 Disabling Host Name Verification

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server (see Chapter 16, "Setting Up Node Manager for an Enterprise Deployment"). If you have not configured the server certificates, you will receive errors when managing the different WebLogic Server instances. To avoid these errors, disable host name verification for the Administration Server and each Managed Server while setting up and validating the topology, and enable it again once the enterprise deployment topology configuration is complete, as described in Chapter 16, "Setting Up Node Manager for an Enterprise Deployment."

You can disable host name verification for a server as soon as it is up and running, starting with the Administration Server.

To disable host name verification:

1. Log in to the WebLogic Server Administration Console.

2. Click **Lock & Edit**.

3. In the **Domain Structure** tree on the left, expand the **Environment** node.

4. Click **Servers**.

5. On the Summary of Servers page, click the name of a server in the **Names** column of the **Servers** table.

6. On the settings page for the server, click the **SSL** tab.

7. Expand the **Advanced** section of the page.

8. Set **Hostname Verification** to None.

9. Click **Save**.

10. Save and activate the changes.

11. This change requires a restart of Node Manager and the Administration Server:

    a. Stop the Administration Server with Node Manager, using the following command:

    ```
    wls:/nm/domain_name>nmKill("AdminServer")
    ```

    b. Stop Node Manager by stopping the process associated with it.

    If it is running in the foreground in a shell, use Ctrl+C.

    If it is running in the background in the shell, find the associated 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
    ```

    c. Start Node Manager:

    ```
    cd WCCUI_WL_HOME/server/bin
    nohup ./startNodeManager.sh > nm.out&
    ```

    In the reference topology, WCCUI_WL_HOME is the /u01/oracle/products/fmw_home/wlserver_10.3 directory.

    d. Start the Administration Server again, as follows:

    * Start the Oracle WebLogic Scripting Tool (WLST):

    ```
    cd WCCUI_ORACLE_COMMON_HOME/common/bin

    ./wlst.sh
    ```

    In the reference topology, WCCUI_ORACLE_COMMON_HOME is the /u01/oracle/products/fmw_home/oracle_common directory.

    * In the WLST shell, connect to Node Manager with the nmConnect command and the Node Manager credentials (make sure Node Manager is up and running), and start Node Manager using nmStart:

    ```
    wls:/offline>nmConnect("node_admin_user","node_admin_password",
    "WCCUIHOST1","5556","domain_name","WCCUI_ASERVER_HOME")
    ```

The values of *node_admin_user* and *node_admin_password* are the Node Manager credentials. For more information about these credentials, see Section 15.5.3.4, "Starting the Administration Server on WCCUIHOST1."

In the reference topology, *WCCUI_ASERVER_HOME* is the `/u01/oracle/config/domains/WCCUIDomain` directory.

* Start the Administration Server using `nmStart`:

```
wls:/nm/domain_name> nmStart("AdminServer")
```

15.5.3.7 Copying the Domain Registry File to the Middleware Home on WCCUIHOST2

As explained in Chapter 4, "Preparing the File System for an Enterprise Deployment," the Middleware home on WCCUIHOST2 is on a separate storage volume (local to WCCUIHOST2) to provide maximum redundancy for the installation binaries volume. The `domain-registry.xml` file created on WCCUIHOST1 during creation of the Administration Server domain is not created on WCCUIHOST2. You need to copy this file from WCCUIHOST1.

To copy the domain registry file from the Middleware home on WCCUIHOST1 to the Middleware home on WCCUIHOST2:

1. Go to the Middleware home directory on WCCUIHOST1.

   ```
   cd WCCUI_MW_HOME
   ```

   In the reference topology, *WCCUI_MW_HOME* is the `/u01/oracle/products/fmw_home` directory.

2. Copy the `domain-registry.xml` file to the Middleware home on WCCUIHOST2, with the following command:

   ```
   scp domain-registry.xml oracle@WCCUIHOST2:WCCUI_MW_HOME
   ```

3. Copy the `nodemanger.domains` file from WCCUIHOST1 to WCCUIHOST2, with the following command:

   ```
   scp WCCUI_WL_HOME/common/nodemanager/nodemanager.domains
   oracle@WCCUIHOST2:WCCUI_WL_HOME/common/nodemanager/
   ```

   In the reference topology, *WCCUI_WL_HOME* is the `/u01/oracle/products/fmw_home/wlserver_10.3` directory.

15.5.4 Registering the WCCUI Managed Servers with MDS and Creating a Metadata Partition

You can register the WCCUI Managed Servers with the Oracle Metadata Services (MDS) Repository through Oracle Enterprise Manager Fusion Middleware Control or through the WebLogic Server Scripting Tool (WLST).

To register the WCCUI Managed Servers with the MDS repository and create the metadata partition through Fusion Middleware Control:

1. Go to Oracle Enterprise Manager Fusion Middleware Control at `http://ADMINVHN:7001/em`.

2. Log in to Fusion Middleware Control with the user name and password you specified in Section 15.5.3.2, "Creating boot.properties for the Administration Server on WCCUIHOST1."

3. Under WebLogic Domain on the left, click WCCUI Domain, then choose Metadata Repositories from the WebLogic Domain menu, as Figure 15–7 shows.

Figure 15–7 WebLogic Domain Menu on WCCUIDomain Page
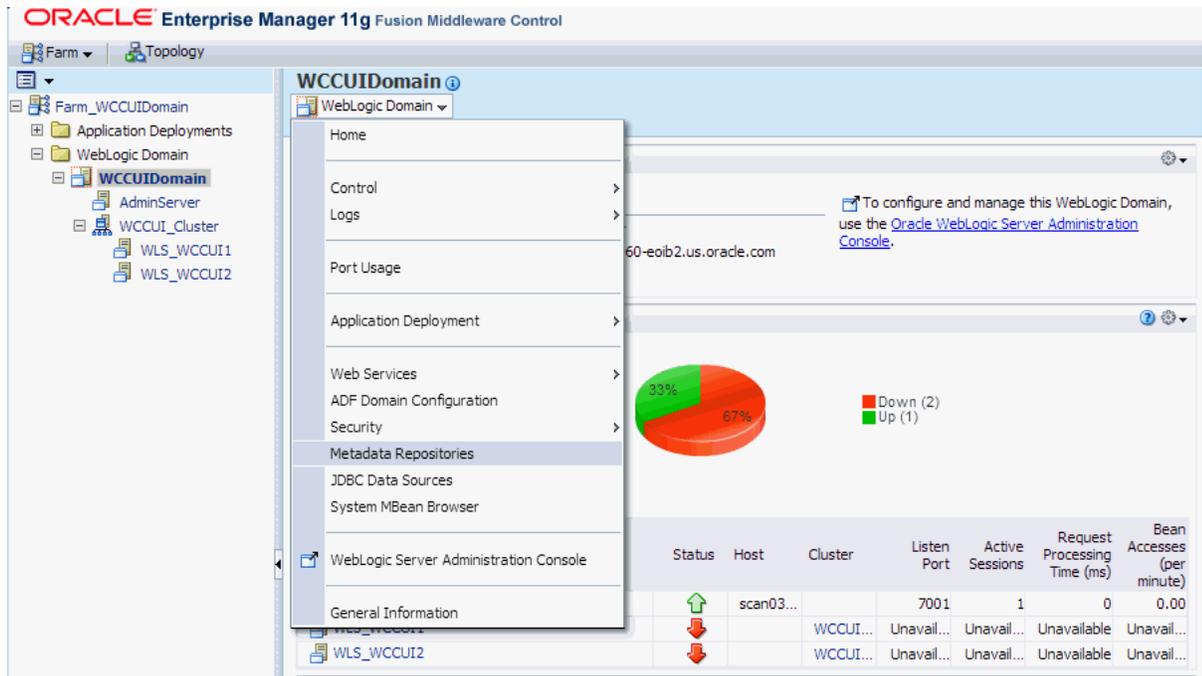
4. On the Metadata Repositories page, click **Register** under **Database-Based Repositories**, as Figure 15–8 shows.

Figure 15–8 Metadata Repositories Page
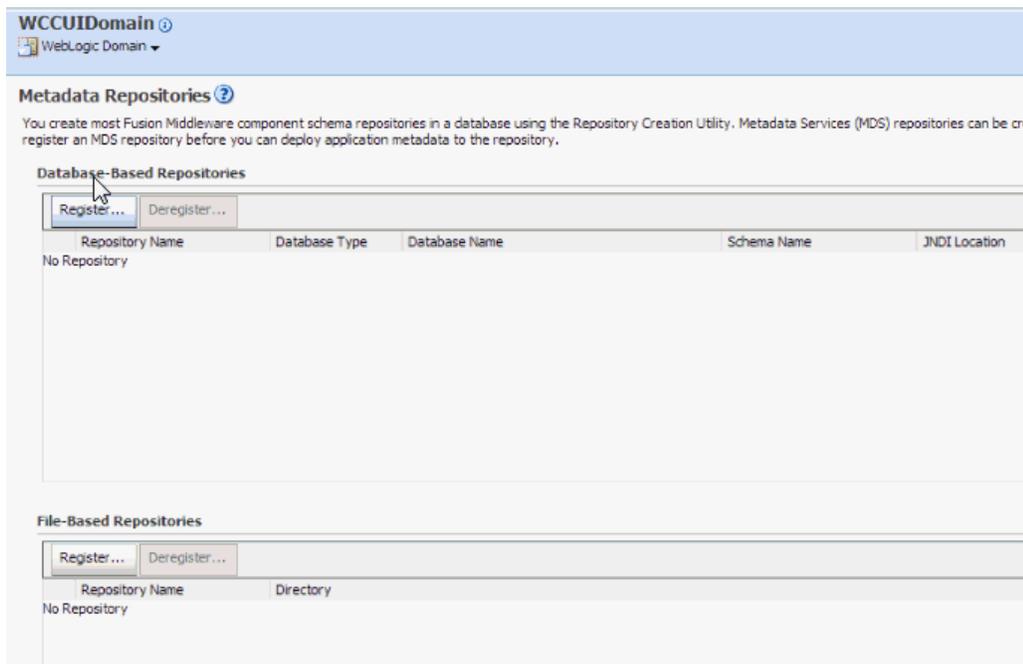
5. Register the MDS repository on the Register Database-Based Metadata Repository page, as Figure 15–9 shows, and then click **OK** on the far right.

Figure 15–9 Register MDS Repository

The Target the Repository dialog box opens.

6. In the Target the Repository dialog box, select **WCCUI_Cluster**, as Figure 15–10 shows, and click **Target**.

Figure 15–10 Target the Repository to WCCUI_Cluster
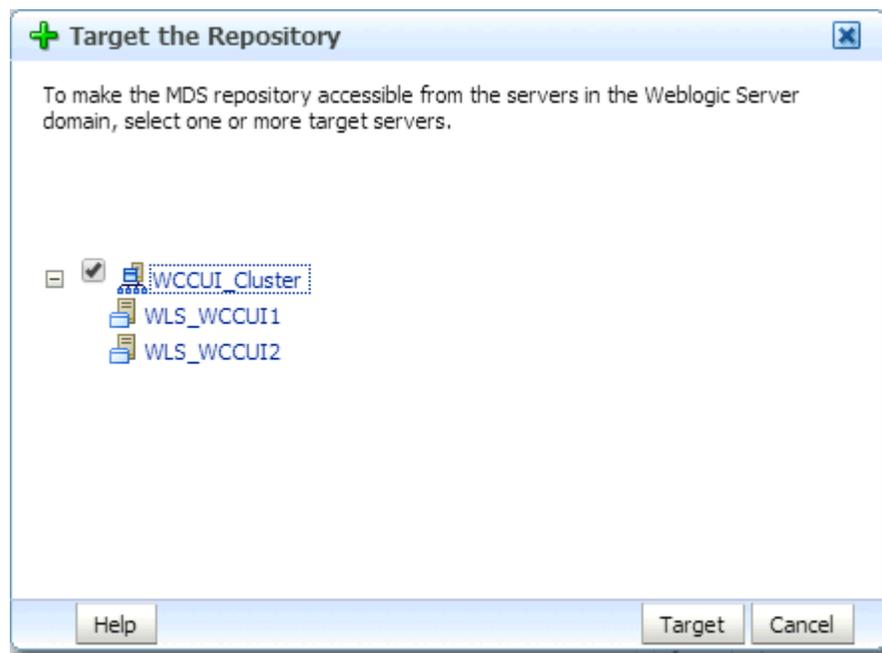
7. Click **Close** when you get the message, `Target operation is completed.`

8. Restart the Administration Server in the WebCenter Content user interface domain, by stopping and then starting it, as described in Section 10.3, "Restarting the Administration Server."

To register the WCCUI Managed Servers with the MDS repository and create the metadata partition through WLST:

1. Run WLST from *WCCUI_MW_HOME*/oracle_common/common/bin/wlst.sh, and connect to the WebLogic Server instance in interactive mode:

```
wls:/offline> connect()
Please enter your username : weblogic
Please enter your password : password

Please enter your server URL: [t3://localhost:7001] :t3://host:port of admin
server where the WebCenter Content user interface Managed Server is running
Connecting to t3://host:7001 with userid weblogic ...
Successfully connected to Admin Server 'AdminServer' that belongs to domain
'WCCUIDomain'.

Warning: An insecure protocol was used to connect to the
server. To ensure on-the-wire security, the SSL port or
Admin port should be used instead.

wls:/WCCUIDomain/serverConfig>
```

In the reference topology, *WCCUI_MW_HOME* is the /u01/oracle/products/fmw_home directory.

2. Run the following command to create a partition:

```
wls:/WCCUIDomain/serverConfig>
createMetadataPartition(repository='mds-WCCUIMDSREPO', partition='MDS_
PARTITION')
Location changed to domainRuntime tree. This is a read-only tree with
DomainMBean as the root.
For more help, use help(domainRuntime)

Executing operation: createMetadataPartition.

Partition "MDS_PARTITION" in Metadata DB repository "mds-WCCUIMDSREPO" was
created successfully.
```

3. Register the MDS repository with the `registerMetadataDBRepository` command:

```
registerMetadataDBRepository('WCCUIMDSREPO', 'Oracle','dbscan.example.com',
'1521', 'wccedg.example.com', 'WCCUI_MDS', 'password', 'WLS_WCCUI1')
```

The target server in the preceding command is the WebCenter Content user interface Managed Server.

The sample `registerMetadataDBRepository` command has these parameters:

■ `WCCUIMDSREPO` is the name of the metadata repository.

■ `oracle` is the database type.

■ `dbscan.example.com` is the name of the database host

■ `1521` is the port number for the database.

■ `wccedg.example.com` is the database service name

- `WCCUI_MDS` is the schema name

- *password* is the password of the schema owner

- `WLS_WCCUI1` is the WebCenter Content user interface Managed Server

4. Restart the Administration Server in the WebCenter Content user interface domain, by stopping and then starting it, as described in Section 10.3, "Restarting the Administration Server."

If you have installed both domains on the same host, the port for the Administration Server in the WebCenter Content user interface domain will *not* be the default Administration Server port.

15.5.5 Propagating the Domain Configuration to WLS_WCCUI1 and WLS_WCCUI2

To propagate the domain configuration to WLS_WCCUI1 and WLS_WCCUI2:

1. Stop the Administration Server.

2. Run the following `pack` command on WCCUIHOST1 to create a template pack:

```
cd WCCUI_ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true -domain=WCCUI_ASERVER_HOME
-template=WCCUIDomainTemplateUI.jar
-template_name=WCCUIDomainTemplateUI
```

In the reference topology, *WCCUI_ORACLE_COMMON_HOME* is the `/u01/oracle/products/fmw_home/oracle_common` directory, and *WCCUI_ASERVER_HOME* is the `/u01/oracle/config/domains/WCCUIDomain` directory.

3. Run the following `unpack` command on WCCUIHOST1 to create the domain directory for the WLS_WCCUI1 Managed Server:

```
cd WCCUI_ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain= WCCUI_MSERVER_HOME -template=WCCUIDomainTemplateUI.jar
-app_dir= WCCUI_APPLICATION_HOME -overwrite_domain=true
```

In the reference topology, *WCCUI_MSERVER_HOME* is the `/u02/oracle/config/domains/WCCUIDomain` directory, and *WCCUI_APPLICATION_HOME* is the `/u01/oracle/config/applications/WCCUIDomain` directory.

Notes:

- Make sure to run `unpack` from the *WCCUI_ORACLE_COMMON_HOME*/common/bin directory, not from *WCCUI_WL_HOME*/common/bin.

- The *WCCUI_APPLICATION_HOME* directory gets backed up with the `unpack` command.

- 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.

---

4. Run the following command on WCCUIHOST1 to copy the template pack created in step 1 to WCCUIHOST2:

```
scp WCCUIDomainTemplateUI.jar oracle@WCCUIHOST2:WCCUI_ORACLE_COMMON_
HOME/common/bin
```

In the reference topology, *WCCUI_ORACLE_COMMON_HOME* is the /u01/oracle/products/fmw_home/oracle_common directory.

5. Run the following unpack command on WCCUIHOST2 to unpack the propagated template to the WLS_WCCUI2 Managed Server domain directory:

```
cd WCCUI_ORACLE_COMMON_HOME/common/bin
```

```
./unpack.sh -domain=/u02/oracle/config/domains/WCCUIDomain
-template=WCCUIDomainTemplateUI.jar
-app_dir=/u01/oracle/config/applications/WCCUIDomain
-overwrite_domain=true
<< read template from "/u01/oracle/products/fmw_home/oracle_
common/common/bin/WCCUIDomainTemplateUI.jar"
>>  succeed: read template from "/u01/oracle/products/fmw_home/oracle_
common/common/bin/WCCUIDomainTemplateUI.jar"
<< set config option OverwriteDomain to "true"
>>  succeed: set config option OverwriteDomain to "true"
<< set config option AppDir to "/u01/oracle/config/applications/WCCUIDomain"
>>  succeed: set config option AppDir to
"/u01/oracle/config/applications/WCCUIDomain"
<< set config option DomainName to "WCCUIDomain"
>>  succeed: set config option DomainName to "WCCUIDomain"
<< write Domain to "/u02/oracle/config/domains/WCCUIDomain"
..................................................................................
...............
>>  succeed: write Domain to "/u02/oracle/config/domains/WCCUIDomain"
<< close template
>>  succeed: close template
```

6. Start Node Manager on WCCUIHOST2, the Administration Server, and the Managed Servers.

15.5.6 Associating the WebCenter Content User Interface with Content Server

Next you need to associate the WebCenter Content user interface with Content Server through the connection architecture.

To associate the WebCenter Content user interface with Content Server:

1. Set the variable *WCCUI_WL_HOME* to the location of the WebLogic Server installation. For example:

```
WCCUI_WL_HOME=WCCUI_MW_HOME/wlserver_10.3
```

In the reference topology, *WCCUI_MW_HOME* is the /u01/oracle/products/fmw_home directory.

2. Go to the following directory:

```
WCCUI_MW_HOME/oracle_common/webcenter/wccadf/ConnArchWlstResources/common/bin
```

3. Run manageconnwlst.sh, a custom WLST script (in the preceding directory):

```
./manageconnwlst.sh
```

```
wls:/offline> connect()
```

```
Please enter your username :weblogic

Please enter your password :

Please enter your server URL [t3://localhost:7001] :t3://WCCUIHOST1:16225

Connecting to t3://WCCUIHOST1:16225 with userid weblogic ...

Successfully connected to managed Server 'WLS_WCCUI1' that belongs to domain
'WCCUIDomain'.


Warning: An insecure protocol was used to connect to the server. To ensure
on-the-wire security, the SSL port or Admin port should be used instead.


wls:/WCCUIDomain/serverConfig>
```

4. Update the RIDC connection to the WebCenter Content user interface Managed Server:

```
wls:/domain_name/serverConfig/updateRIDCConnection('ADF_UI_APP_
NAME','WccAdfDefaultConnection',connUrl='idc://contentserver_host:intradoc_
port',credUsername='ucm_admin_user')
```

In the command, *ADF_UI_APP_NAME* is the **Oracle WebCenter Content - Web UI** application. For example:

```
wls:/WCCUIDomain/serverConfig> updateRIDCConnection('Oracle WebCenter Content -
Web UI', 'WccAdfDefaultConnection',
connUrl='idc://ucminternal.example.com:6300', credUsername='weblogic')
```

> **Note:** In this example, the RIDC connection between the WCCUI and WCC managed servers uses the IDC protocol.
>
> You can also configure a JAX-WS, HTTP, or HTTPS client connection for Oracle WebCenter Content, to associate the WebCenter Content user interface with Content Server. For more information, see "Associating the WebCenter Content User Interface with Content Server" in *Oracle Fusion Middleware Installing and Configuring Oracle WebCenter Content*.

At this point the WebCenter Content user interface application instance has been set up and associated with the WebCenter Content Managed Server that was installed on the first machine.

5. Restart the Content Server Managed Server, using the WebLogic Server Administration Console.

6. Restart the WebCenter Content user interface Managed Server, using the WebLogic Server Administration Console for the WebCenter Content user interface domain.

15.6 Configuring the Administrator User

Content Server and the WebCenter Content user interface will need to access the same user directory. Standard LDAP offerings such as Oracle Internet Directory and Active Directory can be shared across domains. You can choose to configure a single sign-on solution using Oracle Access Manager or Oracle Single Sign-On, using the standard guidelines for such integration.

For more information about LDAP options, see Chapter 8, "Creating a Domain for an Enterprise Deployment."

Out of the box, the WebCenter Content user interface requires one WebCenter Content administrator user to function:

- The administrator user was specified in the `credUsername` parameter of the `updateRIDCConnection()` WLST command that was used to connect to the WebCenter Content user interface Managed Server, in Section 15.5, "Deploying the WebCenter Content User Interface Application to a New Domain," Step 9d.

- You will need a user with the chosen name in the LDAP store or stores. Without this administrator user, the WebCenter Content user interface deployment will not work.

- The user must have `Administrators` rights for the WebCenter Content Managed Server.

15.7 Accessing the WebCenter Content User Interface

You can access the WebCenter Content user interface through the following URL:

```
http://WCCUIHOST1:16225/wcc
```

The WebCenter Content user interface application runs on port 16225 by default.

15.8 Configuring Oracle HTTP Server with the WebCenter Content User Interface Cluster

To enable Oracle HTTP Server to route to WCCUI_Cluster, which contain the WLS_WCCUI1 and WLS_WCCUI2 Managed Servers, you must set the `WebLogicCluster` parameter to the list of nodes in the cluster. Then you can validate access to the Managed Servers through the load balancer.

This section includes the following topics:

- Section 15.8.1, "Configuring Oracle HTTP Server for the WLS_WCCUI Managed Servers"

- Section 15.8.2, "Validating Access Through the Load Balancer"

15.8.1 Configuring Oracle HTTP Server for the WLS_WCCUI Managed Servers

To configure Oracle HTTP Server for the WLS_WCCUI Managed Servers:

1. Create a new file named `wccui_vh.conf` in each of the following directories to define the `<VirtualHost>` directives for the WebCenter Content user interface:

   - `/u02/oracle/config/web1/config/OHS/ohs1/moduleconf`

   - `/u02/oracle/config/web2/config/OHS/ohs2/moduleconf`

2. For each of the web servers on WEBHOST1 and WEBHOST2, add the following lines to the `/u02/oracle/config/web1/config/OHS/ohs1/moduleconf/wccui_vh.conf` and `/u02/oracle/config/web2/config/OHS/ohs2/moduleconf/wccui_vh.conf` files:

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


## Added for external access for WCCUI

# ADF UI
<Location /wcc>
   WebLogicCluster WCCUIHOST1:16225,WCCUIHOST2:16225
   SetHandler weblogic-handler
   WLCookieName WCC-ADF-JSESSIONID
   WLProxySSL ON
   WLProxySSLPassThrough ON
</Location>
```

   In the reference topology, *ORACLE_INSTANCE* is the `/u02/oracle/config/web1` or `/u02/oracle/config/web2` directory.

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

   ORACLE_INSTANCE`/admin/bin/opmnctl restartproc ias-component=ohs`*X*

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

   In the reference topology, *ORACLE_INSTANCE* is the `/u02/oracle/config/web1` or `/u02/oracle/config/web2` directory.

15.8.2 Validating Access Through the Load Balancer

You should verify URLs to ensure that appropriate routing and failover is working from Oracle HTTP Server to WCCUI_Cluster.

To verify the URLs:

1. While WLS_WCCUI2 is running, stop WLS_WCCUI1 from the WebLogic Server Administration Console.

2. Access `http://wcc.example.com/wcc` to verify that it is functioning properly.

3. Start WLS_WCCUI1 from the WebLogic Server Administration Console.

4. Stop WLS_WCCUI2 from the WebLogic Server Administration Console.

5. Access `http://wcc.example.com/wcc` to verify that it is functioning properly.

You can verify the cluster node to which you were directed after the traffic balancing provided through your load balancer and then again through the web tier.

15.9 Completing the Workflow Configuration

To complete the workflow configuration for the WebCenter Content user interface, you need to restart the Managed Servers and verify the configuration. The `UseDatabaseWfInQueue` configuration variable enables the WebCenter Content user interface to filter workflows assigned to a user. The `EmailNotificationType` configuration variable specifies where the links in notification emails point for workflows and subscriptions in different Content Server user interfaces, and its default value is `NativeWebUI`.

To complete the workflow configuration:

1. Make sure that the *WCCUI_DOMAIN*/ucm/cs/config/config.cfg file contains the `EmailNotificationType` variable with either of the following settings:

   - To generate emails with links that point only to the WebCenter Content user interface, set `EmailNotificationType=ContentUI` in `config.cfg`.

   - To generate emails with links that point to both the WebCenter Content user interface and the native 11*g* user interface, set `EmailNotificationType=ContentUI,NativeWebUI` in `config.cfg`.

2. Restart the Content Server Managed Server, using the WebLogic Server Administration Console.

3. Click the alert that appears on the Content Server home page after restart: **Click to complete workflow setup**.

   Ensure that Content Server returns a success message: `The setup for workflow in queue was successful.`

4. Restart the WebCenter Content user interface Managed Server, using the WebLogic Server Administration Console for the WebCenter Content user interface domain.

For more information about workflows, see "Managing Workflows" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

16

Setting Up Node Manager for an Enterprise Deployment

This chapter describes how to configure Node Manager in accordance with the enterprise deployment recommendations.

This chapter includes the following sections:

- Section 16.1, "Overview of Setting Up Node Manager"
- Section 16.2, "Changing the Location of the Node Manager Log"
- Section 16.3, "Enabling Host Name Verification Certificates for Node Manager"
- Section 16.4, "Starting Node Manager"

16.1 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 16–1 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 16–1   Steps for Setting Up Node Manager

Step	Description	More Information
Specify a location for the Node Manager log within the admin directory for the ED.	Edit the `LogFile` property in the `nodemanager.properties` file, and restart Node Manager.	Section 16.2, "Changing the Location of the Node Manager Log"
Set up SSL communication between Node Manager and the Administration Server	Generate self-signed certificates, create identity and trust keystores, configure Node Manager and the Managed Servers to use the custom keystores, and change the host name verification setting for each Managed Server.	Section 16.3, "Enabling Host Name Verification Certificates for Node Manager"
Start Node Manager	Run the `setNMProps.sh` script before starting Node Manager the first time.	Section 16.4, "Starting Node Manager"

Setup Process

The procedures described in this chapter must be performed for various components of the enterprise deployment topology outlined in Section 1.1.1, "Reference Topology Documented in This Guide." Variables are used in this chapter to distinguish between component-specific items:

- *WLS_SERVER*: This variable refers to a WebLogic Server Managed Server for the enterprise deployment component (for example, WLS_WCC1).

- *HOST*: This variable refers to a host machine for the enterprise deployment component (for example, WCCHOST1).

- *VIP*: This variable refers to a virtual IP address for the enterprise deployment component (for example, WCCHOST1VHN1).

The values to be used for these variables are provided in the component-specific chapters in this *Enterprise Deployment Guide*. You must perform the procedures in this chapter multiple times for each host name and virtual IP address pair, using the information provided in Section 10.7, "Configuring Node Manager for the WLS_WCC Managed Servers.".

Recommendations

Oracle provides two main recommendations for Node Manager configuration in enterprise deployment topologies:

1. Oracle recommends placing the Node Manager log file in a location different from the default one (which is inside the Middleware home where Node Manager resides). See Section 16.2, "Changing the Location of the Node Manager Log" for further details.

2. Oracle also recommends using host name verification for communication between Node Manager and the servers in the domain. This requires the use of certificates for the different addresses used in the domain. This chapter explains the steps for configuring certificates in the hosts for host name verification. See Section 16.3, "Enabling Host Name Verification Certificates for Node Manager" for further details.

> **Note:** The passwords used in this guide are used only as examples. Use secure passwords in a production environment. For example, use passwords that consist of random sequences of both uppercase and lowercase characters as well as numbers.

16.2 Changing the Location of the Node Manager Log

To change the location of the Node Manager log, edit the Node Manager properties file, *WL_HOME*/common/nodemanager/nodemanager.properties, and then restart Node Manager.

Add the new location for the log file, using the following line:

```
LogFile=/u02/oracle/config/nodemanager/nodemanager.log
```

Oracle recommends that this location is outside the *MW_HOME* directory and inside the /u02/oracle/config directory for the enterprise deployment topology.

In the reference topology, *WL_HOME* is the /u01/oracle/products/fmw_home/wlserver_10.3 directory, and *MW_HOME* is the /u01/oracle/products/fmw_home directory.

You need to restart Node Manager for this change to take effect.

To restart Node Manager:

1. Stop Node Manager by stopping the process associated with it.

   If it is running in the foreground in a shell, use Ctrl+C.

   If it is running in the background in the shell, find the associated process and use the `kill` command to stop it. For example:

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

   kill -9 9139
   ```

2. Start Node Manager:

   ```
   cd WL_HOME/server/bin
   nohup ./startNodeManager.sh > nm.out&
   ```

   In the reference topology, `WL_HOME` is the `/u01/oracle/products/fmw_home/wlserver_10.3` directory.

16.3 Enabling Host Name Verification Certificates for Node Manager

Setting up SSL for communication between Node Manager and the Administration Server or a Managed Server consists of the following steps:

- Step 1: Generating Self-Signed Certificates Using the utils.CertGen Utility
- Step 2: Creating an Identity Keystore Using the utils.ImportPrivateKey Utility
- Step 3: Creating a Trust Keystore Using the Keytool Utility
- Step 4: Configuring Node Manager to Use the Custom Keystores
- Step 5: Configuring Managed Servers to Use the Custom Keystores
- Step 6: Changing the Host Name Verification Setting for the Managed Servers

16.3.1 Generating Self-Signed Certificates Using the utils.CertGen Utility

The certificates added in this chapter (as an example) address a configuration where Node Manager listens on a physical host name (*HOST*.example.com) and a WebLogic Server Managed Server listens on a virtual host name (*VIP*.example.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.

These certificates should be created using the network name or alias. For information on using trust CA certificates instead, see "Configuring Identity and Trust" in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

The following procedure configures certificates for *HOST*.example.com and *VIP*.example.com. It is assumed that both a physical host name (*HOST*) and a virtual host name (*VIP*) are used in *HOST*. It is also assumed that *HOST*.example.com is the address used by Node Manager, and *VIP*.example.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 an Oracle 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).

To create self-signed certificates on *HOST*:

1. Set up your environment by running the *WL_HOME*/server/bin/setWLSEnv.sh script. In the Bourne shell, run the following commands on *HOST*:

   ```
   cd WL_HOME/server/bin

   . ./setWLSEnv.sh
   ```

   Verify that the *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, WCCHOST2 uses the cert directory created for WCCHOST1 certificates. Create a user-defined directory for the certificates:

   ```
   mkdir cert
   ```

3. Change the 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*.example.com and *VIP*.example.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 password HOST.example.com_cert HOST.example.com_key domestic
   HOST.example.com

   java utils.CertGen password VIP.example.com_cert VIP.example.com_key domestic
   VIP.example.com
   ```

5. If additional host names are used in the same or different nodes, add the required host names to the certificate stores (if they are different from *HOST*.example.com and *VIP*.example.com).

6. If additional host names are used in the same or different nodes, 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).

16.3.2 Creating an Identity Keystore Using the utils.ImportPrivateKey Utility

With the utils.ImportPrivateKey utility, create a new identity keystore.

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, `/u01/oracle/config/domains/WCCDomain/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*`.example.com` and *VIP*`.example.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 password
    appIdentity1 password
    /u01/oracle/config/domains/WCCDomain/cert/HOST.example.com_cert.pem
    /u01/oracle/config/domains/WCCDomain/cert/HOST.example.com_key.pem

    java utils.ImportPrivateKey appIdentityKeyStore.jks password
    appIdentity2 password
    /u01/oracle/config/domains/WCCDomain/cert/VIP.example.com_cert.pem
    /u01/oracle/config/domains/WCCDomain/cert/VIP.example.com_key.pem
    ```

16.3.3 Creating a Trust Keystore Using the Keytool Utility

With the keytool utility, create a new trust keystore.

To create a 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
    /u01/oracle/config/domains/WCCDomain/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 follows:

```
keytool -storepasswd -new New_Password -keystore Trust_Keystore -storepass
Original_Password
```

For example:

```
keytool -storepasswd -new password -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 `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
password
```

16.3.4 Configuring Node Manager to Use the Custom Keystores

To configure Node Manager to use the custom keystores, add the following lines to the end of the `nodemanager.properties` file, located in the *WL_HOME*`/common/nodemanager` directory:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=Identity_Keystore
CustomIdentityKeyStorePassPhrase=Identity_Keystore_Password
CustomIdentityAlias=Identity_Keystore_Alias
CustomIdentityPrivateKeyPassPhrase=Private_Key_Used_When_Creating_Certificate
```

Make sure to use the correct value for `CustomIdentityAlias` on each node; that is, the custom identity alias specifically assigned to that node. For example for WCCHOST2:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=/u01/oracle/config/domains/WCCDomain/cert/appIdenti
tyKeyStore.jks
CustomIdentityKeyStorePassPhrase=password
CustomIdentityAlias=appIdentity2
CustomIdentityPrivateKeyPassPhrase=password
```

The passphrase entries in the nodemanager.properties file get encrypted when you start Node Manager as described in Section 16.4, "Starting Node Manager." For security reasons, you want to minimize the time the entries in the `nodemanager.properties` file are left unencrypted. After you edit the file, you should start Node Manager as soon as possible so that the entries get encrypted.

When using a common, shared storage installation for *MW_HOME*, Node Manager is started from different nodes using the same base configuration (`nodemanager.properties`). In that case, it is required to add the certificate for all the nodes that share the binaries to the `appIdentityKeyStore.jks` identity store. To do this, create the certificate for the new node and import it to `appIdentityKeyStore.jks` as in Section 16.3.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility."

Once the certificates are available in the store, each node manager needs to point to a different identity alias to send the correct certificate to the Administration Server. To do this, set different environment variables 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 WCCHOST1 and `appIdentity2` for WCCHOST2.

16.3.5 Configuring Managed Servers to Use the Custom Keystores

With the Oracle WebLogic Server Administration Console, configure Managed Servers to use the identity and trust keystores.

To configure Managed Servers to use the custom keystores:

1. Log in to the Oracle WebLogic Server Administration Console.

2. Click **Lock & Edit**.

3. Expand the **Environment** node in the **Domain Structure** tree on the left.

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:

     ```
     /u01/oracle/config/domains/WCCDomain/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 16.3.3, "Creating a Trust Keystore Using the Keytool Utility." This attribute is optional or required depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server reads only from the keystore, so whether or not you define this property depends on the requirements of the keystore.

9. In the Trust section, define properties for the trust keystore:

- **Custom Trust Keystore:** The fully qualified path to the trust keystore:

  `/u01/oracle/config/domains/WCCDomain/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 16.3.3, "Creating a Trust Keystore Using the Keytool Utility." This attribute is optional or required depending on the type of keystore. All keystores require the passphrase to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server reads only from the keystore, so whether or not you define this property depends on the requirements of the keystore.

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 16.3.2, "Creating an Identity Keystore Using the utils.ImportPrivateKey Utility."

15. Click **Save**.

16. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.

17. Restart the server for which the changes have been applied, using the Administration Console.

16.3.6 Changing the Host Name Verification Setting for the Managed Servers

Once the steps above have been performed, you should set host name verification for the affected Managed Servers to `Bea Host Name Verifier`.

To change the host name verification setting for the Managed Servers:

1. Log in to the WebLogic Server Administration Console.

2. Expand the **Environment** node in the **Domain Structure** tree on the left.

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, using the Administration Console.

16.4 Starting Node Manager

Run the following commands 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 8.4.2, "Starting Node Manager on WCCHOST1," to enable the use of the start script for your Managed Servers.

```
cd WL_HOME/server/bin

export JAVA_OPTIONS=-DCustomIdentityAlias=appIdentityX

nohup ./startNodeManager.sh > nm.out&
```

Notes:

■ Make sure to specify the custom identity alias specifically assigned to each host, so `appIdentity1` for WCCHOST1 and `appIdentity2` for WCCHOST2.

■ It is assumed that any other pertaining Java options are passed to Node Manager in each node. For example, for WCCHOST1, which hosts the Administration Server, also include `-DDomainRegistrationEnabled=` along with `-DCustomIdentityAlias=` in the `JAVA_OPTIONS` parameter.

■ Verify that Node Manager is using the appropriate stores and alias from the Node Manager output, which should be as follows:

```
CustomIdentityKeyStoreFileName=
ASERVER_HOME/certs/appIdentityKeyStore.jks
CustomIdentityAlias=appIdentityX
```

In the reference topology, *ASERVER_HOME* is the `/u01/oracle/config/domains/WCCDomain` directory.

Host name verification works if you apply a test configuration change to the servers, and it succeeds without Node Manager reporting any SSL errors.

17

Configuring Server Migration for an Enterprise Deployment

This chapter describes the procedures for configuring server migration for an enterprise deployment.

This chapter includes the following sections:

- Section 17.1, "Overview of Server Migration for an Enterprise Deployment"
- Section 17.2, "Setting Up a User and Tablespace for the Server Migration leasing Table"
- Section 17.3, "Creating a GridLink Data Source for leasing Using the Administration Console"
- Section 17.4, "Editing Node Manager's Properties File"
- Section 17.5, "Setting Environment and Superuser Privileges for the wlsifconfig.sh Script"
- Section 17.6, "Configuring Server Migration Targets"
- Section 17.7, "Testing the Server Migration"

17.1 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 IP addresses that are failed over by 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 1.1.1, "Reference Topology Documented in This Guide."

Variables are used in this chapter to distinguish between component-specific items:

- *WLS_SERVER1* and *WLS_SERVER2* refer to the 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 WebLogic Server migration.

Table 17–1 describes the steps for configuring server migration for the WebLogic Server Managed Servers.

Table 17–1   Steps for Configuring Server Migration

Step	Description	More Information
Set up a user, tablespace, and migration table	Create a `leasing` tablespace, user, and table for server migration.	Section 17.2, "Setting Up a User and Tablespace for the Server Migration leasing Table"
Create GridLink data sources for the `leasing` table	Create a data source for each of the Oracle RAC database instances and the global `leasing` GridLink data source in the Administration Console.	Section 17.3, "Creating a GridLink Data Source for leasing Using the Administration Console"
Specify Node Manager properties values for migration	Edit the property values in the `nodemanager.properties` file for each host, and verify the values.	Section 17.4, "Editing Node Manager's Properties File"
Set the environment and specify superuser privileges for the oracle user	Add files to the `PATH` environment variable, and grant the `sudo` privilege for the `wlsifconfig.sh` script.	Section 17.5, "Setting Environment and Superuser Privileges for the wlsifconfig.sh Script"
Configure cluster migration	Assign available nodes as migration targets, and specify candidate machines for each server.	Section 17.6, "Configuring Server Migration Targets"
Test server migration	Verify server migration between hosts from Node Manager or the Administration Console.	Section 17.7, "Testing the Server Migration"

17.2 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 table `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 password;

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;
   ```
   d. Commit the changes in the database

   ```
   SQL> commit;
   ```

17.3 Creating a GridLink Data Source for leasing Using the Administration Console

Create a GridLink data source for the `leasing` table from the Oracle WebLogic Server Administration Console.

To create a GridLink data source:

1. Log in to the 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**, select **GridLink Data Source**, and perform the following steps:

    -   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. On the Transaction Options screen, clear **Supports Global Transactions**, and click **Next**.

6. On 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.example.com
        ```

    -   **Host Name and Port**: Enter the SCAN address and port for the RAC database being used, and click **Add**. 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.example.com
        ```

        > **Note:**   For Oracle Database 11g, use the virtual IP address and port of each database instance listener, as in these examples:
        >
        > ```
        > wccdbhost1-vip.example.com (port 1521)
        >
        > wccdbhost2-vip.example.com (1521)
        > ```

    -   **Database User Name**: `leasing`

- **Password**: Enter the password for the `leasing` user.

- **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.example.com)
(PORT=1521)))(CONNECT_DATA=(SERVICE_NAME=wccedg.example.com))) succeeded.
```

Click **Next**.

9. In the ONS Client Configuration page, perform the following steps:

- Select **FAN Enabled** to subscribe to and process Oracle FAN events.

- Enter the host names for the RAC database and the ONS remote port, as reported by the database, and click **ADD**:

  The following example displays the number of the ONS remote port:

  ```
  [orcl@db-scan1 ~]$ srvctl config nodeapps -s

  ONS exists: Local port 6100, remote port 6200, EM port 2016
  ```

- Click **Next**.

  > **Note:** For Oracle Database 11*g*, use the host name and port of each database's ONS service, as in these examples:
  >
  > ```
  > wccdbhost1.example.com (port 6200)
  >
  > wccdbhost2.example.com (6200)
  > ```

10. On the Test ONS Client Configuration s, review the connection parameters, and click **Test All ONS Nodes**.

    Here is an example of a successful connection notification:

    ```
    Connection test for db-scan.example.com:6200 succeeded.
    ```

    Click **Next**.

11. In the Select Targets page, select the targets for which you are doing server migration, **IMG_Cluster**, **CPT_Cluster**, **SOA_Cluster**, and **All Servers in the cluster**.

12. Click **Finish**.

13. Click **Activate Changes**.

17.4 Editing Node Manager's Properties File

The third step is to edit the Node Manager properties file. This needs to be done for Node Manager 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 address (for example, `eth0`).

  Do not specify the subinterface, such as `eth0:1` or `eth0:2`. This interface is to be used without `:0` or `:1`. The Node Manager scripts traverse the different `:X`-enabled IP addresses to determine which to add or remove. For example, the valid values in Linux environments are `eth0`, `eth1`, `eth2`, `eth3`, and `ethn`, depending on the number of interfaces configured.

- **NetMask:** This property specifies the net mask for the interface for the floating IP address. The net mask should 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 the Node Manager output (shell where Node Manager is started) that these properties are being used, or problems might 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 following step is not required if the server properties (start properties) have been properly set and Node Manager can start the servers remotely.

- 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.

> **Note:** When you run Node Manager from a shared storage installation, multiple nodes are started using the same `nodemanager.properties` file. Each node, however, may require different NetMask or Interface properties. In this case, specify individual properties 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
> ```
>
> Start Node Manager after the variable has been set in the shell.
>
> For each node, you can include other Java options that specify properties to pass to Node Manager. For example, for WCCHOST1, which hosts the Administration Server, include `-DDomainRegistrationEnabled=` along with `-DCustomIdentityAlias=` in the `JAVA_OPTIONS` parameter.

17.5 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):

To set environment and superuser privileges for the script:

1. Ensure that your `PATH` environment variable includes the files listed in Table 17–2.

Table 17–2   Files Required for the PATH Environment Variable

File	Located in This Directory
`wlsifconfig.sh`	`/u02/oracle/config/domains/WCCDomain/bin/server_migration/`
`wlscontrol.sh`	*WL_HOME*`/common/bin/`
`nodemanager.domains`	*WL_HOME*`/common/nodemanager/`

2. Grant the `sudo` privilege 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 the `sudo` privilege to the WebLogic Server 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 Server user (`oracle`). The following is an example of an entry inside `/etc/sudoers` granting the `sudo` execution privilege for `oracle` and also over `ifconfig` and `arping`:

     ```
     oracle ALL=NOPASSWD: /sbin/ifconfig,/sbin/arping
     ```

> **Note:** Ask the system administrator for the `sudo` and `system` privileges as appropriate for this step.

3. Start Node Manager on *HOST1* and *HOST2* by running the `startNodeManager.sh` script, which is located in the *WL_HOME*`/server/bin/` directory:

```
nohup ./startNodeManager.sh > nm.out&
```

17.6 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.

To configure cluster migration in a migration in a cluster:

1. Log in to the WebLogic Server Administration Console (`http//ADMINVHN:7001/console`).

2. In the **Domain Structure** tree on the left, 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 Imaging, Capture, and Oracle SOA Suite 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** tree on the left of the WebLogic Server Administration Console, expand **Environment** and select **Servers**.

    b. Select the server for which you want to configure migration.

    > **Note:** For the procedures in this document, configure server migration for the Imaging, Capture, and Oracle SOA Suite clusters.

    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 Node Manager, the Administration Server, and the servers for which server migration has been configured:

        * First, stop the Managed Servers through the Administration Console.

        * Then restart the Node Manager and Administration Server, as described in step 11 under Section 8.4.5, "Disabling Host Name Verification,"

        * Finally, start the Managed Servers again, through the Administration Console.

17.7 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*:

```
kill -9 pid
```

where `pid` specifies the process ID of the Managed Server. You can identify the process ID in the node by running this command:

```
ps -ef | grep WLS_SERVER1
```

2. Watch the Node Manager console. You should see a message indicating that `WLS_SERVER1`'s floating IP address 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.

To verify that server migration is working properly 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 address for `WLS_SERVER1` is being brought up and that the server is being restarted in this node.

2. Access your server's console in the same IP address.

To verify that server migration is working properly from the Administration Console

1. Log in to the Administration Console.

2. Click **Domain** on the left.

3. Click the **Monitoring** tab and then the **Migration** subtab.

The Migration Status table provides information on the status of the migration (Figure 17–1).

Figure 17–1   Migration Status Screen in the Administration Console
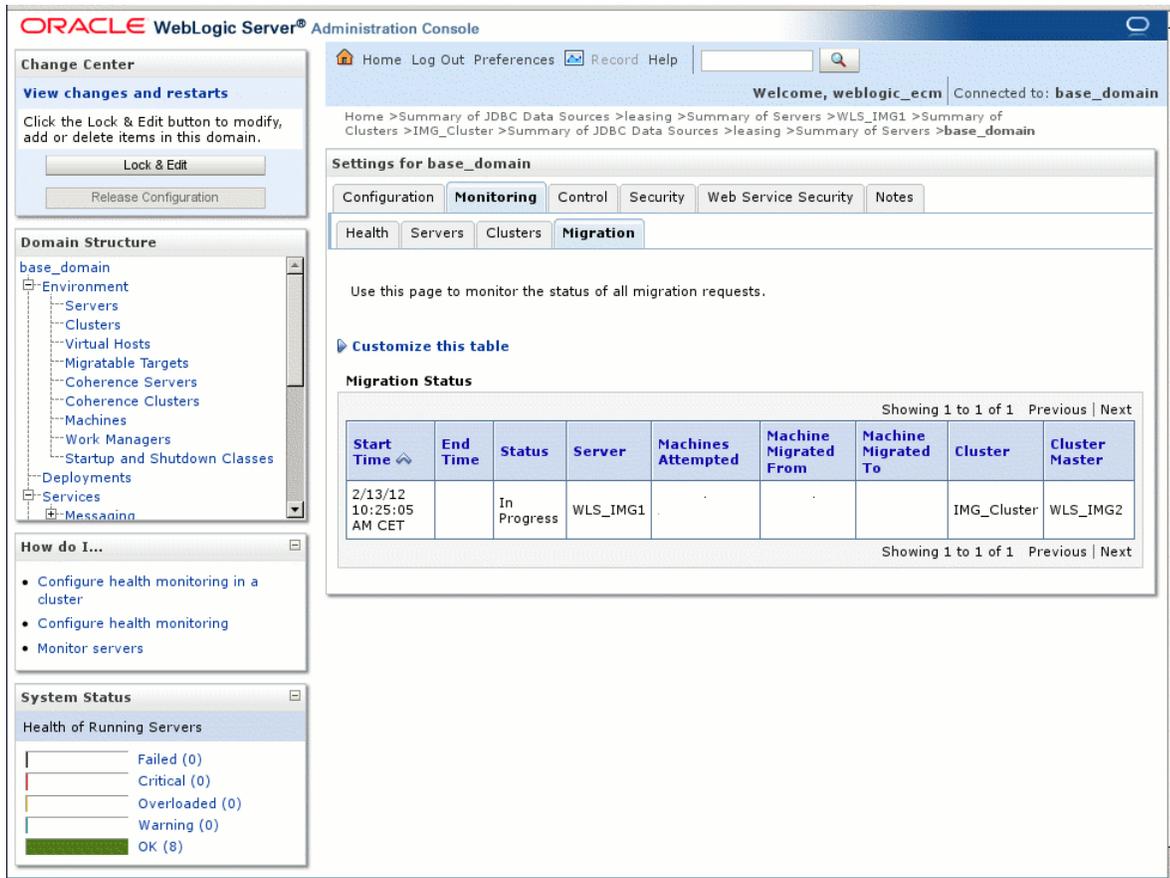
> **Note:**   After a server is migrated, to fail it back to its original node or machine, stop the Managed Server from the WebLogic Server Administration Console and then start it again. The appropriate Node Manager will start the Managed Server on the machine to which it was originally assigned.

18

Integrating with Oracle Identity Management

This chapter describes how to integrate Oracle WebCenter Content with Oracle Identity Management.

This chapter includes the following sections:

- Section 18.1, "Overview of Integrating with Oracle Identity Management"
- Section 18.2, "Reassociating the Identity Store with an External LDAP Authentication Provider"
- Section 18.3, "Integrating with Oracle Access Manager 11g"
- Section 18.4, "Validating Access Through the Load Balancer and SSO"
- Section 18.5, "Backing Up the Installation"

18.1 Overview of Integrating with Oracle Identity Management

Oracle Access Manager is the recommended single sign-on solution for Oracle Fusion Middleware 11g Release 1. You can integrate an Oracle Fusion Middleware enterprise deployment with Oracle Identity Management 11g. The following sections describe how to integrate the policy store and identity store for the Oracle WebCenter Content domain with Oracle Identity Management.

> **Note:** When integrating with Oracle Identity Management, use the transport mode currently in use by the Oracle Access Management servers; for example, `Open`, `Simple`, or `Cert`.

Table 18–1 lists the high-level steps for integrating Oracle Identity Management 11g with an Oracle WebCenter Content enterprise deployment.

Table 18–1   Steps for Integrating with Oracle Identity Management 11g

Step	Description	More Information
Register the WebGate agent	Register the WebGate agent using the RREG tool.	Section 18.3.3, "Registering the WebGate Agent"
Install and configure WebGate	Install WebGate on each of the WEBHOST machines, where Oracle HTTP Server has already been installed.	Section 18.3.4, "Setting Up WebGate"
Set up WebLogic Server authentication providers	Set up the WebLogic Server authentication providers by backing up the configuration files, setting up the Oracle Access Manager identity assertion provider, and setting the order of providers.	Section 18.3.6, "Setting Up the WebLogic Server Authentication Providers"
Reassociate the identity store with Oracle Internet Directory or another external LDAP authentication provider.	Configure Oracle Internet Directory, Oracle Virtual Directory, or a third-party LDAP authentication provider as the identity store for the domain. Add the `weblogic_ecm` administration user to use for setting up the rest of the enterprise deployment topology.	Section 18.2, "Reassociating the Identity Store with an External LDAP Authentication Provider"

18.2 Reassociating the Identity Store with an External LDAP Authentication Provider

The following sections describe how to reassociate the identity store from the Oracle WebLogic Server default embedded LDAP store with Oracle Internet Directory, Oracle Virtual Directory, or a third-party external LDAP authentication provider:

- Section 18.2.1, "Backing Up Configuration Files"

- Section 18.2.2, "Creating the LDAP Authentication Provider"

- Section 18.2.3, "Setting the Order of Providers"

- Section 18.2.4, "Moving the WebLogic Server Administrator to the LDAP Identity Store"

- Section 18.2.5, "Resetting Imaging Security for the New Identity Store"

18.2.1 Backing Up Configuration Files

To be safe, before you create the LDAP authentication provider, you should first back up the relevant configuration files:

```
ASERVER_HOME/config/config.xml
ASERVER_HOME/config/fmwconfig/jps-config.xml
ASERVER_HOME/config/fmwconfig/system-jazn-data.xml
```

Also back up the boot properties file for the Administration Server:

```
ASERVER_HOME/servers/AdminServer/security/boot.properties
```

In the reference topology, *ASERVER_HOME* is the `/u01/oracle/config/domains/WCCDomain` directory.

18.2.2 Creating the LDAP Authentication Provider

You can use the Oracle WebLogic Server Administration Console to set up the proper authenticator.

To create the LDAP authentication provider:

1. Log in to the Administration Console.

2. Click the **Security Realms** link on the left.

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** for Oracle Internet Directory.

9. Select the **OracleInternetDirectoryAuthenticator** type from the list of authenticators.

10. Click **OK**.

11. On 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 `DefaultAuthenticator` and set it 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.

Parameter	Value	Value Description
Host	For example: `oid.example.com`	The LDAP server's server ID.
Port	For example: `636`	The LDAP server's port number.
Principal	For example: `cn=orcladmin`	The LDAP user DN used to connect to the LDAP server.
Credential	NA	The password used to connect to the LDAP server.
SSL Enabled	Checked	Specifies whether SSL protocol is used when connecting to LDAP server.
User Base DN	For example: `cn=Users,dc=us, dc=example,dc=com`	Specify the DN under which your Users start.

Parameter	Value	Value Description
Group Base DN	For example: `cn=Groups,dc=us, dc=example,dc=com`	Specify the DN that points to your `Groups` node.
Use Retrieved User Name as Principal	Checked	Must be turned on.

Click **Save** when done.

16. Click **Activate Changes** to propagate the changes.

18.2.3 Setting the Order of Providers

Reorder the Oracle Internet Directory Authenticator and Default Authenticator, and ensure that the control flag for each authenticator is set in the following order:

- Oracle Internet Directory 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. Click **Reorder** and ensure that the control flags for the Oracle Internet Directory Authenticator, and Default Authenticator are set as follows:

- Oracle Internet Directory LDAP Authenticator: **SUFFICIENT**

- Default Authenticator: **SUFFICIENT**

Note: Enterprise Capture authorization will not work correctly unless the Authentication Provider is set as **SUFFICIENT**.

---

5. Click **Save**.

6. Click **Activate Changes** to propagate the changes.

7. Restart the Administration Server, as described in Section 10.3, "Restarting the Administration Server," and all Managed Servers in the domain.

To restart the Managed Servers, stop all of them before you restart the Administration Server, and start them after you restart it.

18.2.4 Moving the WebLogic Server Administrator to the LDAP Identity Store

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 18.2.4.1, "Provisioning Administrator Users and Groups in an LDAP Directory"

- Section 18.2.4.2, "Assigning the Admin Role to the Admin Group"

- Section 18.2.4.3, "Updating the boot.properties File and Restarting the System"

18.2.4.1 Provisioning Administrator 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. After setting up and testing the entire enterprise deployment topology, you might want to set up a different system administrator with appropriate roles for each application.

For setting up the Oracle WebCenter Content WebLogic Server domain, provision a new system administrator named `weblogic_ecm` in the LDAP identity store with the following DNs:

- Admin User DN:

  ```
  cn=weblogic_ecm,cn=Users,dc=us,dc=example,dc=com
  ```

- Admin Group DN:

  ```
  cn=ECM Administrators,cn=Groups,dc=us,dc=example,dc=com
  ```

To provision the administration user and administration group in Oracle Internet Directory:

1. Create an LDIF file named `admin_user.ldif` with the following contents, and then save the file:

   ```
   dn: cn=weblogic_ecm, cn=Users, dc=us, dc=example, dc=com
   orclsamaccountname: weblogic_ecm
   givenname: weblogic_ecm
   sn: weblogic_ecm
   userpassword: password
   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.example.com -p 389 -D "cn=orcladmin" -w password
   -c -v -f PATH/admin_user.ldif
   ```

3. Create an LDIF file named `admin_group.ldif` with the following contents, and then save the file:

```
dn: cn=ECM Administrators, cn=Groups, dc=us, dc=example, dc=com
displayname: ECM Administrators
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
uniquemember: cn=weblogic_ecm, cn=Users, dc=us, dc=example, 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.example.com -p 389 -D "cn=orcladmin"
-w password -c -v -f PATH/admin_group.ldif_file
```

5. Create an LDIF file named `administrators_group.ldif` with the following contents, and then save the file:

```
dn: cn=Administrators, cn=Groups, dc=us, dc=example, dc=com
displayname: Default WLS Administrators
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
cn: Administrators
description: WL Administrators Group
```

> **Note:** Create the Administrators group only if it does not exist in Oracle Internet Directory.

6. Run the `ldapadd` command on the Oracle Internet Directory host located under the *ORACLE_HOME*/bin directory to provision the Administrators group in Oracle Internet Directory:

```
ORACLE_HOME/bin/ldapadd -h oid.example.com -p 389 -D "cn=orcladmin" -w password
-c -v -f PATH/administrators_group.ldif
```

7. Create an LDIF file named `modify_administrators_group.ldif` with the following contents, and then save the file:

```
dn: cn=Administrators, cn=Groups, dc=us, dc=example, dc=com
changetype: modify
add: uniqueMember
uniqueMember: cn=ECM Administrators, cn=Groups, dc=us, dc=example, dc=com
```

8. Run the `ldapmodify` command on the Oracle Internet Directory host located under the *ORACLE_HOME*/bin directory to modify the Administrators group in Oracle Internet Directory:

```
ORACLE_HOME/bin/ldapmodify -h oid.example.com -p 389 -D "cn=orcladmin" -w
password -c -v -f PATH/modify_administrators_group.ldif
```

18.2.4.2 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.

To assign the Admin role to the Admin group:

1. Log in to the WebLogic Server Administration Server Console.

2. In the navigation tree on the left, 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 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 WebCenter Content applications 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.

18.2.4.3 Updating the boot.properties File and Restarting the System

The `boot.properties` file for the Administration Server should be updated with `weblogic_ecm`, the WebLogic Server administration user created in Oracle Internet Directory.

To update the `boot.properties` file:

1. On WCCHOST1, go the following directory:

   ```
   cd ASERVER_HOME/servers/AdminServer/security
   ```

   In the reference topology, `ASERVER_HOME` is the `/u01/oracle/config/domains/WCCDomain` directory.

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=password
   ```

4. Save the file.

5. Restart the Administration Server, as described in Section 10.3, "Restarting the Administration Server."

18.2.5 Resetting Imaging Security for the New Identity Store

If you have already configured your Imaging Managed Server and you change the LDAP provider, the global user IDs (GUIDs) in the Imaging security tables will be invalid. Imaging caches the GUIDs from an external LDAP provider in its local security tables and uses these IDs for authentication. You can refresh the GUID values in the Imaging security tables with WLST commands or with Oracle Enterprise Manager Fusion Middleware Control.

Only users and groups that exist in both LDAP providers will have GUIDs refreshed. Imaging permissions assigned to users and groups from the previous LDAP will be refreshed to the users and groups that match in the new LDAP. The `refreshIPMSecurity` command will ignore any users or groups that do not match any users or groups in the new LDAP provider.

> **Note:** During the refresh, users or groups for whom matching identifying information is not found are ignored. As security changes are made, invalid users or groups are removed from the Imaging database.

18.2.5.1 Refreshing GUID values in Imaging Security Tables with WLST

If you want to refresh GUID values from a command line, you can use the Oracle WebLogic Scripting Tool (WLST).

To refresh GUID values in Imaging security tables with WLST:

1. Start the Administration Server for your Oracle WebLogic Server domain, as described in Section 8.4.3, "Starting the Administration Server on WCCHOST1."

2. Log in to WCCHOST1, where the Administration Server is running.

3. Navigate to the Oracle WebCenter Content home directory: *MW_HOME/WCC_ORACLE_HOME*.

4. Invoke WLST:

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

5. Connect to the Imaging Managed Servers:

```
wls:/offline> connect()
Please enter your username :weblogic_ecm
Please enter your password : XXXXXXXXXXXXX
Please enter your server URL [t3://localhost:7001]
 : t3://WCCHOST1VHN2:16000
Connecting to t3://WCCHOST1VHN2:16000 with userid weblogic_ecm ...
Successfully connected to Managed Server 'WLS_IMG1' that belongs to domain
'domainName'.

Warning: An insecure protocol was used to connect to the
server. To ensure on-the-wire security, the SSL port or
Admin port should be used instead.

wls:/domainName/serverConfig> listIPMConfig()   <This is just to check
that the connection is to the right Imaging server>

wls:/domainName/serverConfig>
refreshIPMSecurity()  <This is the command that will refresh the GUIDs in the
Security tables.>

wls:/domainName/serverConfig> exit()
```

6. Log in to Imaging to verify user and group security.

18.2.5.2 Refreshing GUID values in Imaging Security Tables with Fusion Middleware Control

If you want to refresh GUID values through an MBean, you can use the System MBean Browser in Fusion Middleware Control.

To refresh GUID values in Imaging security tables with Fusion Middleware Control:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control for `WCCdomain`:

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

2. In the navigation tree on the left, expand **WebLogic Domain**, then the Oracle WebCenter Content domain folder, then **IMG_Cluster**, and then the name of the Imaging server, such as **WLS_IMG1**.

3. On the right, click the **WebLogic Server** drop-down menu, and choose **System MBean Browser**.

4. In the System MBean Browser navigation tree, expand **Application Defined MBeans**, then **oracle.imaging**, then **Server: WLS_IMG1**, and then **cmd**, and click **cmd**.

5. Click **refreshIPMSecurity** on the right, under the **Operations** tab.

6. Click the **Invoke** button.

7. Log in to Imaging to verify user and group security.

18.2.6 Adding a System Administrator in LDAP with Enterprise Capture Roles

In an LDAP-integrated system, you need to assign the Oracle Enterprise Capture Roles to the new system administrator user (`weblogic_ecm`) so this user can perform the Enterprise Capture Administrator role.

To add a system administrator in LDAP with Enterprise Capture roles:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control.

2. On the left, expand **WebLogic Domain**.

3. Right-click the domain name, choose **Security**, and then choose **Application Roles**.

   The Application Roles page opens.

4. In the **Application Stripe** field, choose **capture** from the drop-down list, and then click the search icon.

   The search populates the table with roles for the Capture User, Capture Workspace Manager, and Capture Viewer.

5. Edit the **CaptureWorkspaceManager** role, and add `weblogic_ecm` to this role.

6. Edit the **CaptureUser** role, and add `weblogic_ecm` to this role, so that it has both the **CaptureWorkspaceManager** and **CaptureUser** roles.

18.3 Integrating with Oracle Access Manager 11g

This section describes how to set up Oracle Access Manager 11*g* as the single sign-on solution for the Oracle WebCenter Content enterprise deployment topology. It contains the following sections:

- Section 18.3.1, "Overview of Oracle Access Manager Integration"

- Section 18.3.2, "Prerequisites for Oracle Access Manager"

- Section 18.3.3, "Registering the WebGate Agent"

- Section 18.3.4, "Setting Up WebGate"

- Section 18.3.5, "Copying Files and Artifacts Generated from OAM WebGate Registration to the Webgate Instance Location"

- Section 18.3.6, "Setting Up the WebLogic Server Authentication Providers"

18.3.1 Overview of Oracle Access Manager Integration

This section explains the procedure for configuring the Oracle WebCenter Content installation with an existing Oracle Access Manager 11*g* installation, with Oracle Internet Directory as the underlying directory service. For more information about installing and configuring an Oracle Access Manager installation, see the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management*.

> **Note:** The Oracle WebCenter Content enterprise deployment
> topology described in this guide uses a single sign-on configuration in
> which both the Oracle WebCenter Content system and the single
> sign-on system are in the same network domain (`example.com`). For a
> multidomain configuration, see the required configuration steps in
> "Introduction to the OAM Policy Model, Single Sign-On" in the *Oracle
> Fusion Middleware Administrator's Guide for Oracle Access Manager with
> Oracle Security Token Service.*

18.3.2 Prerequisites for Oracle Access Manager

The setup for Oracle Access Manager assumes an existing Oracle Access Manager 11*g*
installation. 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 Oracle Internet Directory as the
directory service.

In addition, the Oracle Access Manager installation should have its own web server
configured with WebGate.

18.3.3 Registering the WebGate Agent

This section describes the procedures for registering the WebGate agent with Oracle
Access Manager and the use of WebGate agent instances on each of the WEBHOST
machines:

- Section 18.3.3.1, "Extracting and Using the RREG Tool"

- Section 18.3.3.2, "Updating the Oracle Access Manager 11g Request File"

- Section 18.3.3.3, "Running the oamreg Tool"

- Section 18.3.3.4, "Changing the inspection.wsil Resource to Use the Basic
  Authentication Scheme"

- Section 18.3.3.5, "Updating the Oracle Access Manager 11g Server Configuration to
  Support the Basic Cookieless Scheme"

18.3.3.1 Extracting and Using the RREG Tool

The RREG tool is part of the Oracle Access Manager 11*g* installation. If it is not already
available, extract it on each of the Oracle Identity Management machines.

To extract the RREG tool:

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 -xzvf RREG.tar
   ```

3. Open the *RREG_HOME*/bin/oamreg.sh script, and change the `OAM_REG_HOME`
   parameter according to your setup, if necessary.

The RREG Configuration Tool provides a way to register WebCenter Content resources in the Oracle Access Manager system.

You need to add these resources to the Oracle Access Manager system:

```
/adfAuthentication
/imaging/faces
/ibr/adfAuthentication
/em
/console
/DefaultToDoTaskFlow
/sdpmessaging/userprefs-ui
/integration/worklistapp
/workflow/sdpmessagingsca-ui-worklist
/soa/composer
/soa-infra
/soa-infra/deployer
/soa-infra/events/edn-db-log
/soa-infra/cluster/info
/dc-console/adfAuthentication
/dc-client/adfAuthentication
/wcc/adfAuthentication
```

The list of public resources follows:

```
/cs
/_ocsh
/imaging
/_dav
/soa-infra/directWSDL
/dc-console
/dc-client
/wcc
```

The list of excluded resources follows:

```
/idcnativews
/imaging/ws
/imaging/lib
/cs/common/idcapplet.jar
/cs/images
/wsm-pm
/soa-infra/services
/ucs/messaging/webservice
/axf-ws
```

> **Note:** These lists of resources are applicable to Oracle Access Manager 11.1.2.1.0. If you are using Oracle Access Manager 11.1.2.2.0, you need to move /dc-client to the excluded resources list.

18.3.3.2 Updating the Oracle Access Manager 11g Request File

The *RREG_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>/ibr/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/sdpmessagingsca-ui-worklist</resource>
        <resource>/soa/composer</resource>
        <resource>/soa-infra/deployer</resource>
        <resource>/soa-infra/events/edn-db-log</resource>
        <resource>/soa-infra/cluster/info</resource>
        <resource>/soa-infra</resource>
        <resource>/dc-console/adfAuthentication</resource>
        <resource>/dc-client/adfAuthentication</resource>
        <resource>/wcc/adfAuthentication</resource>
    </protectedResourcesList>
    <publicResourcesList>
        <resource>/cs</resource>
        <resource>/_ocsh</resource>
        <resource>/_dav</resource>
        <resource>/imaging</resource>
        <resource>/soa-infra/directWSDL</resource>
        <resource>/dc-console</resource>
        <resource>/dc-client</resource>
        <resource>/wcc</resource>
    </publicResourcesList>
    <excludedResourcesList>
        <resource>/wsm-pm</resource>
        <resource>/soa-infra/services</resource>
        <resource>/ucs/messaging/webservice</resource>
        <resource>/imaging/ws</resource>
        <resource>/idcnativews</resource>
        <resource>/imaging/lib</resource>
        <resource>/cs/common/idcapplet.jar</resource>
        <resource>/cs/images</resource>
        <resource>/axf-ws</resource>
    </excludedResourcesList>
```

```
                         <userDefinedParameters>
                             <userDefinedParam>
                                 <name>filterOAMAuthnCookie</name>
                                 <value>false</value>
                             </userDefinedParam>
                         </userDefinedParameters>

</OAM11GRegRequest>
```

Notes:

- The contents of this file are applicable to Oracle Access Manager 11.1.2.1.0. If you are using Oracle Access Manager 11.1.2.2.0, you need to move /dc-client to the excluded resources list.

- The *resource_name*/.../* resources will be automatically added during the registration.

- This guide describes the validation field entry in request files for Oracle Access Manager 11*g* (11.1.1.2) and later. The validation exception list is defined differently in earlier versions of Oracle Access Manager 11*g*. For earlier versions, instead of using the <ValList> entry as shown in the preceding text, use the following syntax after the </publicResourcesList> entry.

```
            <userDefinedParameters>
                <userDefinedParam>
                    <name>ipValidationExceptions</name>
                    <value>10.1.1.1</value>
                </userDefinedParam>
            </userDefinedParameters>
```

For more information about adding validation exceptions, see the *Oracle Fusion Middleware Administrator's Guide for Oracle Access Manager with Oracle Security Token Service.*

18.3.3.3 Running the oamreg Tool

Run the oamreg tool with the following command:

```
$ ./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: MW_HOME/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.example.com:7001
---------------------------------------

Inband registration process completed successfully! Output artifacts are created
in the output folder.
```

18.3.3.4 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.

To change the `inspection.wsil` resource to use the basic authentication scheme:

1. Log in to the Oracle Access Manager console at `http://`*OAM_HOST*`:`*OAM_ADMINSERVER_PORT*`/oamconsole`.

2. Using the navigation tree on the left, click **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.

4. Expand **Authentication Policies**.

5. 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**.

6. 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 13.5.13, "Configuring a BPEL CSF Credential" for further details. (This book uses the `weblogic_ecm` user as an example for SSO.)

18.3.3.5 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 11*g* configuration to `true` on each of the OAMHOST machines. To do this, edit the `oam-config.xml` file located in the *IDM_Home*/oam/server/config/ directory, and change the line

```
<Setting Name="NoUniqueSessionsFor10gAgents" Type="xsd:string">false</Setting>
```

to

```
<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.

18.3.4 Setting Up WebGate

You must set up WebGate on each of the WEBHOST machines where Oracle HTTP Server has already been installed.

This section covers the following topics:

- Section 18.3.4.1, "Installing GCC Libraries"

- Section 18.3.4.2, "Installing WebGate"

- Section 18.3.4.3, "Postinstallation Steps"

18.3.4.1 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 website:

http://gcc.gnu.org

> **Note:** The setup in this guide uses Oracle Identity and Access Management 11*g* (11.1.1.6.0). For version 11.1.1.7.0 or later, installation of third-party GCC libraries is not necessary.

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 18–2 lists the versions of third-party GCC libraries for Linux and Solaris operating systems.

Table 18–2   Versions of GCC Third-Party Libraries for Linux and Solaris Systems

Operating System	Architecture	GCC Libraries	Required Library Version
Linux 32-bit	x86	libgcc_s.so.1 libstdc++.so.5	3.3.2
Linux 64-bit	x64	libgcc_s.so.1 libstdc++.so.6	3.4.6
Solaris 64-bit	SPARC	libgcc_s.so.1 libstdc++.so.5	3.3.2

18.3.4.2 Installing WebGate

This section describes the procedures for installing WebGate. You must install WebGate on each of the WEBHOST machines.

18.3.4.2.1 Launching the Installer The installer program for Oracle HTTP Server 11*g* WebGate for Oracle Access Manager is included in the `webgate.zip` file.

To launch 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 *MW_HOME* environment variable to the Middleware home for Oracle Web Tier:

   ```
   export MW_HOME=/u02/oracle/products/fmw_home
   ```

4. Start the installer using the following command:

   ```
   $ ./runInstaller -jreLoc WT_ORACLE_HOME/jdk
   ```

   In the command, *WT_ORACLE_HOME*=/u02/oracle/products/fmw_home/web_home.

   > **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.

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

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

3. On the Specify Installation Location screen, specify the **Oracle Middleware Home** and **Oracle Home Directory** locations:

   - *MW_HOME*
   - `webgate_home`

   > **Note:** The Middleware home contains an Oracle home for Oracle Web Tier.

   Click **Next**.

4. On 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 18.3.4.1, "Installing GCC Libraries"), and click **Next**.

   > **Note:** This step is not required for WebGate version 11.1.1.7.0 or later.

5. On the Installation Summary screen, verify the information on this screen and click **Install** to begin the installation.

6. On 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. On the Installation Complete screen, click **Finish** to exit the installer.

18.3.4.3 Postinstallation Steps

Complete the following procedure on each of the WEBHOST machines after installing Oracle HTTP Server 11*g* WebGate for Oracle Access Manager.

To do postinstallation steps:

1. Move to the following directory under your Oracle home for WebGate:

   ```
   $ cd WEBGATE_ORACLE_HOME/webgate/ohs/tools/deploy
   ```

   In the reference topology, `WEBGATE_ORACLE_HOME` is the `/u02/oracle/products/fmw_home/webgate_home` directory. This directory is where you installed Oracle HTTP Server WebGate and created the Oracle home for WebGate.

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 /u02/oracle/config/webN/config/OHS/ohsN/
   -oh WEBGATE_ORACLE_HOME
   ```

   The `/u02/oracle/config/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 `WT_ORACLE_HOME`/lib:

   ```
   $ export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/u02/oracle/products/fmw_home/web_
   home/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_RACLE_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 /u02/oracle/config/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. This directory is the Oracle home for WebGate; for example:

```
/u02/oracle/products/fmw_home/webgate_home
```

The `/u02/oracle/config/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
```

18.3.5 Copying Files and Artifacts Generated from OAM WebGate Registration to the Webgate Instance Location

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_
INSTANCE/config/OHS/ohsN/webgate/config/
```

```
scp cwallet.sso oracle@WEBHOSTN:ORACLE_INSTANCE/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`.

In the reference topology, `ORACLE_INSTANCE` is the `/u02/oracle/config/web1` or `/u02/oracle/config/web2` directory.

18.3.6 Setting Up the WebLogic Server Authentication Providers

This section is based on the assumption that you have already set up the LDAP authentication provider by following the steps in Section 18.2.2, "Creating the LDAP Authentication Provider." If you have not already created the LDAP authentication provider, do it before continuing with this section.

This section covers the following topics:

- Section 18.3.6.1, "Backing Up Configuration Files"

- Section 18.3.6.2, "Setting Up the Oracle Access Manager Identity Assertion Provider"

- Section 18.3.6.3, "Setting the Order of Providers"

18.3.6.1 Backing Up Configuration Files

To be safe, first back up the relevant configuration files:

```
ASERVER_HOME/config/config.xml
ASERVER_HOME/config/fmwconfig/jps-config.xml
ASERVER_HOME/config/fwmconfig/system-jazn-data.xml
```

In the reference topology, *ASERVER_HOME* is the
`/u01/oracle/config/domains/WCCDomain` directory.

In addition, back up the `boot.properties` file for the Administration Server.

18.3.6.2 Setting Up the Oracle Access Manager Identity Assertion Provider

Set up an Oracle Access Manager identity assertion provider in the Oracle WebLogic
Server Administration Console.

To set up the Oracle Access Manager identity assertion provider:

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 the asserter type **OAMIdentityAsserter** from the
    drop-down 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 assertion provider.

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.

10. Log in to the Oracle WebLogic Scripting Tool (WLST) as an administrator, and run
    the `addOAMSSOProvider` command:

    a. Start WLST:

    ```
    cd ORACLE_COMMON_HOME/common/bin

    ./wlst.sh
    ```

    b. Connect to the `WCCDomain` Administration Server and issue the
        `addOAMSSOProvider` command:

    ```
    wls:/offline> connect('weblogic_ecm', password,'ADMINVHN:7001')

    Connecting to t3://ADMINVHN:7001 with userid weblogic_ecm ..

    Successfully connected to Admin Server 'AdminServer' that belongs to domain
    'WCCDomain'.

    Warning: An insecure protocol was used to connect to the server. To ensure
    on-the-wire security, the SSL port or Admin port should be used instead.
    ```

```
wls:/WCCDomain/serverConfig>
addOAMSSOProvider(loginuri="/${app.context}/adfAuthentication",logouturi="/
oamsso/logout.html",autologinuri="/obrar.cgi")

Location changed to domainRuntime tree. This is a read-only tree with
DomainMBean as the root.
For more help, use help(domainRuntime)

wls:/WCCDomain/serverConfig> exit()


Exiting WebLogic Scripting Tool
```

18.3.6.3 Setting the Order of Providers

Set the order of identity assertion and authentication providers in the WebLogic Server Administration Console.

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 assertion provider, the Oracle Internet Directory authentication provider, and the default authentication provider by ensuring that the control flag for each provider is set as follows:

   - Oracle Access Manager identity assertion provider: REQUIRED

   - Oracle Internet Directory authentication provider: SUFFICIENT

   - `DefaultAuthenticator`: SUFFICIENT

5. Click **OK**.

6. Click **Activate Changes** to propagate the changes.

7. Restart the Administration Server and all Managed Servers.

   Stop the Administration Server with the `nmKill` command, or with the Administration Console, and then starting it with the `nmStart` command, as described in Section 10.3, "Restarting the Administration Server."

   Before the restart, stop all Managed Servers in the domain through the Administration Console, and then start them after the restart. Log in to the Administration Console using the credentials for the `weblogic_ecm` user.

18.4 Validating Access Through the Load Balancer and SSO

Validate single sign-on through the front end (using the SSO user name and password):

- `http://admin.example.com/console`

- `http://admin.example.com/em`

- `http://wcc.example.com/cs`

- `http://wcc.example.com/imaging`

- `https://wcc.example.com/dc-console`

18.5 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 *Administrator's Guide* provides further details. For information about describing the Oracle HTTP Server data that must be backed up and restored, see the "Backup and Recovery Recommendations for Oracle HTTP Server" section in this 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. For information about database backup, see the *Oracle Database Backup and Recovery User's Guide*.

To back up the installation at this point:

1. Back up Oracle Web Tier:

    a. Shut down the instance using `opmnctl`:

    ```
    /u02/oracle/config/webN/bin/opmnctl stopall
    ```

    b. Back up the Middleware home for Oracle Web Tier with the following command (as root):

    ```
    tar -cvpf BACKUP_LOCATION/web_home.tar $MW_HOME
    ```

    c. Back up the Instance Home for Oracle Web Tier with the following command (as root):

    ```
    tar -cvpf BACKUP_LOCATION/web_instance.tar $ORACLE_INSTANCE
    ```

    d. Start the instance with `opmnctl`:

    ```
    /u02/oracle/config/webN/bin/opmnctl startall
    ```

    In the reference topology, `ORACLE_INSTANCE` is the `/u02/oracle/config/web1` or `/u02/oracle/config/web2` directory.

2. Back up the AdminServer domain directory on WCCHOST1. Perform a backup to save your domain configuration. The configuration files all exist under the `/u01/oracle/config/domains/WCCDomain` directory.

    ```
    tar -cvpf edgdomainback.tar /u01/oracle/config/domains/WCCDomain
    ```

19

Managing the Topology for an Enterprise Deployment

This chapter describes some operations that you can perform after you have set up the topology, including monitoring, scaling, and backing up your topology.

This chapter includes the following sections:

19.1 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 19–1 lists some tasks you can perform to manage the topology.

Table 19–1   Tasks for Managing the Oracle WebCenter Content Topology

Task	Description	More Information
Configure Imaging for high performance, scalability, and high availability in an Imaging cluster	Define an optimal input file strategy.	Section 19.2, "Defining an Optimal Input File Strategy for Imaging"
Manage the Oracle SOA Suite subsystem used by Imaging	Deploy SOA composites to a server address, manage space in the Oracle SOA Suite infrastructure, and configure UMS drivers.	Section 19.3, "Deploying Composites and Artifacts in the Oracle WebCenter Content Enterprise Deployment Topology" Section 19.4, "Managing Space in the SOA Infrastructure Database" Section 19.5, "Configuring UMS Drivers for Oracle WebCenter Content: Imaging"
Expand the topology by scaling it up, or out	Add new Managed Servers to nodes, or add new nodes.	Section 19.6, "Scaling Up the Oracle WebCenter Content Topology" Section 19.7, "Scaling Out the Oracle WebCenter Content Topology"
Back up the topology before and after any configuration changes	Back up directories and files to protect against failure as a result of configuration changes.	Section 19.9, "Performing Backups and Recoveries in Oracle WebCenter Content Enterprise Deployments"
Prevent connection timeouts	Configure the firewall so that the database connection is not timed out.	Section 19.11, "Preventing Timeouts for SQLNet Connections"
Configure Oracle Web Services Manager (Oracle WSM) security policies for Oracle WebCenter Content and Oracle WebCenter Content: Imaging web services	Use the appropriate Oracle WSM policy enforcements instead of basic HTTP authentication.	Section 19.12, "Configuring Oracle Web Service Manager Security Policies for Oracle WebCenter Content and Imaging Services"
Troubleshoot problems	Implement solutions for known issues that may occur after you have configured the topology.	Section 19.13, "Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology"

For more information about managing Oracle WebCenter Content, see the following documents:

- *Administering Oracle WebCenter Enterprise Capture*

- *Administering Oracle WebCenter Content*

- *Oracle Fusion Middleware Administering Oracle WebCenter Content: Imaging*

- *Managing Oracle WebCenter Content*

19.2 Defining an Optimal Input File Strategy for 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 through 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 through the Work Manager created within the Imaging deployment.

Optimum performance will be achieved as follows:

- Each Imaging cluster instance has the maximum affordable number of parsing agents configured through 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.

19.3 Deploying Composites and Artifacts in the Oracle WebCenter Content Enterprise Deployment Topology

When deploying SOA composites to the Oracle SOA Suite subsystem used by Imaging, deploy to a specific server's address and not to the load balancer address (`wcc.example.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.

19.4 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 Oracle Enterprise Manager Fusion Middleware Control (dashboard for instances). Search also in the Oracle SOA Suite server's logs for errors, such as this one:

```
Error Code: 1691
...
ORA-01691: unable to extend lob segment
SOAINFRA.SYS_LOB0000108469C00017$$ by 128 in tablespace SOAINFRA
```

These messages are typically indicators of space issues in the database that may likely require adding more data files or more space to the existing files. The SOA database administrator should determine the extension policy and parameters to be used when adding space. Additionally, old composite instances can be purged to reduce the SOA infrastructure database size. Oracle does not recommend using Fusion Middleware Control for this type of operation because in most cases such operations cause a transaction timeout.

For more details on the possible operations included in the SQL packages provided, see "Deploying and Managing SOA Composite Applications" in the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*. Always use the scripts provided for a correct purge. Deleting rows in just the `composite_dn` table may leave dangling references in other tables used by the Oracle SOA Suite infrastructure.

19.5 Configuring UMS Drivers for Oracle WebCenter Content: Imaging

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, you need to configure the UMS drivers.

> **Note:** This step is required only if the Oracle SOA Suite system used by Oracle WebCenter Content: Imaging is using Unified Messaging System (UMS).

To configure UMS drivers for Imaging:

1. Apply the configuration of UMS drivers in each and every one of the servers in the enterprise deployment 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 follows:

   ```
   /u02/oracle/config/domains/WCCDomain/servers/server_name/
   tmp/_WL_user/ums_driver_name/*/configuration/driverconfig.xml
   ```

   In the command, * 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 WCCHOST1.

2. Force a failover of WLS_IMG1 to WCCHOST2. Verify the directory structure for the UMS driver configuration in the failover node:

   ```
   cd /u02/oracle/config/domains/WCCDomain/servers/server_name/
   tmp/_WL_user/ums_driver_name/*/configuration
   ```

   In the command, * represents a directory whose name is randomly generated by WLS during deployment; for example, `3682yq`).

3. Run the following command on WCCHOST1 to do a remote copy of the driver configuration file from WCCHOST1 to WCCHOST2:

```
scp /u02/oracle/config/domains/WCCDomain/servers/server_name/
tmp/_WL_user/ums_driver_name/*/configuration/
driverconfig.xml
oracle@WCCHOST2:/u02/oracle/config/domains/WCCDomain/servers/server_name/tmp/_
WL_user/ums_driver_name/*/configuration/
```

In the command, `*` represents a directory whose name is randomly generated by Oracle WebLogic Server during deployment; for example, `3682yq`.

It is required to restart the driver for these changes to take effect (that is, for the driver to consume the modified configuration).

To restart the driver:

1. Log in to the WebLogic Server Administration Console.

2. Expand the **Environment** node in 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.

Verify in Fusion Middleware Control that the properties for the driver have been preserved.

19.6 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 a Middleware home in shared storage. Use these existing installations (such as WebLogic Server home, 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`.

> **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-up procedure depends on the topology component:

- Section 19.6.1, "Scale-Up Procedure for WebCenter Content"
- Section 19.6.2, "Scale-Up Procedure for Oracle WebCenter Content: Imaging"
- Section 19.6.3, "Scale-Up Procedure for Oracle WebCenter Enterprise Capture"
- Section 19.6.4, "Scale-Up Procedure for Oracle SOA Suite"

19.6.1 Scale-Up Procedure for WebCenter Content

Only one WebCenter Content Managed Server per node per domain is supported by Oracle Fusion Middleware. To add additional WebCenter Content Managed Servers, follow the steps in Section 19.7.1, "Scale-Out Procedure for WebCenter Content" to add a WebCenter Content Managed Server to a new node.

19.6.2 Scale-Up Procedure for Oracle WebCenter Content: Imaging

Before scaling up the Imaging servers, you must enable a virtual IP address on WCCHOST1 (say, WCCHOST1VHN2), and you must also correctly resolve the host names in the network system used by the topology (with either DNS server or host resolution). For information about how to enable the virtual IP addresses, see Section 10.7, "Configuring Node Manager for the WLS_WCC Managed Servers."

To scale up the Imaging servers in the enterprise deployment topology:

1. Using the 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 address 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_IMG*n* in the summary of servers.

   The remainder of the steps that follow are based on the assumption that you are adding a new server to WCCHOST1, which is already running WLS_IMG1.

2. Configure JMS persistence stores and JMS servers 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 Imaging are configured with no persistence store and use the WebLogic Server store (`/u02/oracle/config/domains/WCCDomain/servers/server_name/data/store/default`).

You must change each Oracle JMS server persistence 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 click **Create FileStore**.

e. On the Create a New File Store page, enter the following information:

- **Name:** `IMGJMSServerNStore` (for example, `IMGJMSServer3Store`, which allows you identify the service it is created for)

- **Target:** `WLS_IMGn` (for example, `WLS_IMG3`).

- **Directory:** Specify a directory that is located in shared storage so that it is accessible from both WCCHOST1 and WCCHOST2 (`/u01/oracle/config/domains/WCCDomain/IMG_Cluster/jms`).

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:** `IpmJmsServern` (for example, `IpmJmsServer3`)

- **Persistent Store:** select the persistence store that you created earlier: **IMGJMSServer*N*Store** (for example, **IMGJMSServer3Store**).

Click **Next**, and then specify `WLS_IMGn` (for example, `WLS_IMG3`) as the target.

i. Click **Finish**, and then activate the changes.

3. Configure a default persistence store for WLS_IMG*n* 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_IMG*n*** (represented as a hyperlink) in the **Name** column of the table. The settings page for the WLS_IMG*n* server opens with the **Configuration** tab active.

d. Click the **Services** tab.

e. Click **Lock & Edit**.

f. Click **Save**, and activate the changes.

4. Disable host name verification for the new Managed Server, as described in Section 8.4.5, "Disabling Host Name Verification," if not already disabled.

Before you can start and verify the WLS_IMG*n* Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for communication between the Administration Server and Node Manager in WCCHOST*n*. If host name verification was already disabled on the source server from which the new one has been cloned, then these steps are not required (the host name verification setting is propagated to the cloned server).

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*n* Managed Servers in the cluster.

   d. Ensure that the newly created Managed Server, WLS_IMG*n*, is running.

6. Add the host name of the WLS_IMG*n* Managed Server (WCCHOST*n*VHN2) to the `SocketHostNameSecurityFilter` parameter list:

   a. Open the file `/u01/oracle/config/domains/WCCDomain/WCC_ Cluster/cs/config/config.cfg` in a text editor.

   b. Add the WLS_IMG*n* Managed Server listen addresses to the list of addresses that are allowed to connect to Oracle WebCenter Content:
   `SocketHostNameSecurityFilter=localhost|localhost.example.com|WCCHOS T1|WCCHOST2|WCCHOST`*n*`VHN`*n*

   c. Save the modified `config.cfg` file, and restart the Oracle WebCenter Content servers for the changes to take effect, using the WebLogic Server Administration Console.

7. Verify that server migration is configured 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, so the following steps are only for verification. The floating IP address for the new Imaging Managed Server should also be already present.

To verify that server migration is configured:

   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. Verify that the **Automatic Server Migration Enabled** option is selected.

This option enables Node Manager to start a failed server on the target node automatically.

g. Click **Save**.

h. Restart Node Manager, the Administration Server, and the servers for which server migration has been configured:

* First, stop the Managed Servers through the Administration Console.

* Then restart the Node Manager and Administration Server, as described in step 11 under Section 8.4.5, "Disabling Host Name Verification,"

* Finally, start the Managed Servers again, through the Administration Console.

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_IMG*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_IMGn
  ```

- Watch the Node Manager Console for a message indicating that WLS_IMG*n*'s floating IP address has been disabled.

- Wait for Node Manager to attempt a second restart of WLS_IMG*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 WebLogic Server 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.

19.6.3 Scale-Up Procedure for Oracle WebCenter Enterprise Capture

Before scaling up the Oracle WebCenter Enterprise Capture servers, you must enable a virtual IP address on WCCHOST1 (say, WCCHOST1VHN3), and you must also correctly resolve the host names in the network system used by the topology (with either DNS server or host resolution). For information about how to enable the virtual IP addresses, see Section 10.7, "Configuring Node Manager for the WLS_WCC Managed Servers."

To scale up the Capture servers in the enterprise deployment topology:

1. Using the WebLogic Server Administration Console, clone WLS_CPT1 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_CPT1**).

   c. Click **Clone**.

   d. Name the new Managed Server WLS_CPTn, where n is a number that identifies the new Managed Server.

   e. For the server listen address, assign the host name or IP address 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 Capture cluster (CPT_Cluster). The reference topology in this book uses port number 16400.

   g. Click **OK** and **Activate Changes**. You should now see the newly created server WLS_CPTn in the summary of servers.

   The remainder of the steps that follow are based on the assumption that you are adding a new server to WCCHOST1, which is already running WLS_CPT1.

2. Configure JMS persistence stores and JMS servers for Capture.

   Configure the location for the JMS persistence stores as a directory that is visible from both nodes. By default, the JMS servers used by Capture are configured with no persistence store and use the WebLogic Server store (`/u01/oracle/config/domains/WCCDomain/servers/server_name/data/store/default`).

   You must change each Oracle JMS server persistence 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:** CPTJMSServer$n$Store (for example, CPTJMSServer3Store, which enables you to identify the service it is created for)

   - **Target:** WLS_CPTn (for example, WLS_CPT3).

   - **Directory:** Specify a directory that is located in shared storage so that it is accessible from both WCCHOST1 and WCCHOST2 (`/u01/oracle/config/domains/WCCDomain/CPT_Cluster/jms`).

    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:** `CaptureJmsServer`n (for example, `CaptureJmsServer3`)

       - **Persistent Store:** Select the persistence store that you created earlier: **CPTJMSServer$n$Store** (for example, **CPTJMSServer3Store**).

       Click **Next**, and then specify `WLS_CPT`n (for example, `WLS_CPT3`) as the target

    i.   Click **Finish**, and activate the changes.

3. Configure a default persistence store for CPTn 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 **CPT_IMGn** (represented as a hyperlink) in the **Name** column of the table. The settings page for the CPT_IMGn server opens with the **Configuration** tab active.

    d. Click the **Services** tab.

    e. Click **Lock & Edit**.

    f.   Click **Save** and activate the changes.

4. Disable host name verification for the new Managed Server, as described in Section 8.4.5, "Disabling Host Name Verification," if not already disabled.

    Before you can start and verify the CPT_IMGn Managed Server, you must disable host name verification. You can reenable it after you have configured server certificates for communication between the Administration Server and Node Manager in WCCHOSTn. If host name verification was already disabled on the source server from which the new one has been cloned, then these steps are not required (the host name verification setting is propagated to the cloned server).

5. Start the newly created Managed Server (WLS_CPT):

    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_CPTn Managed Servers in the cluster.

    d. Ensure that the newly created Managed Server, WLS_CPTn, is running.

6. Add the host name of the WLS_CPTn Managed Server (WCCHOSTnVHN3) to the `SocketHostNameSecurityFilter` parameter list:

    a. Open the file `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs/config/config.cfg` in a text editor.

    b. Add the WLS_CPTn Managed Server listen addresses to the list of addresses that are allowed to connect to Oracle WebCenter Content:
`SocketHostNameSecurityFilter=localhost|localhost.example.com|WCCHOST1|WCCHOST2|WCCHOST`n`VHN`n

    c. Save the modified `config.cfg` file, and restart the Oracle WebCenter Content servers for the changes to take effect, using the WebLogic Server Administration Console.

7. Verify that server migration is configured 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, so the following steps are only for verification. The floating IP address for the new Imaging Managed Server should also be already present.

To verify that server migration is configured:

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 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 Migration Configuration section, select the servers that participate in migration in the **Available** window, and then 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_CPT1, select WCCHOST2. For new Managed Servers on WCCHOST2, which is already running WLS_CPT2, select WCCHOST1.

> **Note:** The appropriate resources must be available to run the Managed Servers concurrently during migration.

f. Verify that the **Automatic Server Migration Enabled** option is selected.

This option enables Node Manager to start a failed server on the target node automatically.

g. Click **Save**.

h. Restart Node Manager, the Administration Server, and the servers for which server migration has been configured:

    * First, stop the Managed Servers through the Administration Console.

    * Then restart the Node Manager and Administration Server, as described in step 11 under Section 8.4.5, "Disabling Host Name Verification,"

    * Finally, start the Managed Servers again, through the Administration Console.

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_CPT*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_IMGn
   ```

   ■ Watch the Node Manager Console for a message indicating that WLS_CPT*n*'s floating IP address has been disabled.

   ■ Wait for Node Manager to attempt a second restart of WLS_CPT*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 WebLogic Server 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.

19.6.4 Scale-Up Procedure for Oracle SOA Suite

Before scaling up the Imaging servers, you must enable a virtual IP address on WCCHOST1 (say, WCCHOST1VHN1), and you must also correctly resolve the host names in the network system used by the topology (with either DNS server or host resolution). For information about how to enable the virtual IP addresses, see Section 10.7, "Configuring Node Manager for the WLS_WCC Managed Servers."

> **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.

To scale up the Oracle SOA Suite servers in the enterprise deployment topology:

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_SOA*n*, where *n* is a number that identifies the new Managed Server.

> **Note:** The remainder of the steps are based on the assumption that you are adding a new server to WCCHOST1, which is already running WLS_SOA1.

2. For the listen address, assign the host name or IP address to use for this new Managed Server. If you are planning to use server migration for this server (which Oracle recommends), this should be the virtual IP address (also called a floating IP address) to enable it to move to another node. The virtual IP address 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 persistence 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 4.4, "Recommended Locations for Different Directories":

   `/u01/oracle/config/domains/WCCDomain/SOA_Cluster/jms/`

   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 UMSJMSServer (for example, `UMSJMSFileStore_N`). Specify the path for the store. This should be a directory on shared storage, as recommended in Section 4.4, "Recommended Locations for Different Directories":

   `/u01/oracle/config/domains/WCCDomain/SOA_Cluster/jms/`

   > **Note:** You can also assign `SOAJMSFileStore_N` as the store for the new UMS JMS servers. For the purpose of clarity and isolation, individual persistence stores are used in the following steps.

   d. Create a new JMS server for UMS (for example, UMSJMSServer_N). Use `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 **Domain Structure** tree on the left of the WebLogic Server Administration Console, and then expand the **Messaging** node. Click **JMS Modules**. The JMS Modules page opens. Click **SOAJMSModule** (represented as a hyperlink in the Names column of the table). The Settings page for SOAJMSModule opens. Open the **SubDeployments** tab, which shows information about the subdeployment module for SOAJMS.

   > **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 **SOAJMSServer*XXXXXX*** 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 **Domain Structure** tree on the left of the WebLogic Server Administration Console and then expand the **Messaging** node. Click **JMS Modules**. The JMS Modules page opens. Click **UMSJMSSystemResource** (represented as a hyperlink in the Names column of the table). The Settings page for UMSJMSSystemResource opens. Open the **SubDeployments** tab, which shows information about the subdeployment module for UMSJMS.

> **Note:** This subdeployment module name is a random name in the form of `UCMJMSServer`*`XXXXXX`* resulting from the Configuration Wizard JMS configuration for the first two servers (WLS_SOA1 and WLS_SOA2).

Click the **UMSJMSServer*XXXXXX*** 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 12.5, "Configuring Oracle Coherence for Deploying Composites."

> **Note:** Only the `localhost` field needs to be changed for the server. Replace the `localhost` value with the listen address of the new server added:
>
> `Dtangosol.coherence.localhost=SOAHOST1VHN`*`n`*.

5. Configure a Tx persistence store for the new server. This should be a location visible from other nodes as indicated in the recommendations about shared storage (see Section 4.4, "Recommended Locations for 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 persistence store to store its data files:

`/u01/oracle/config/domains/WCCDomain/SOA_Cluster/tlogs`

6. Disable host name verification for the new Managed Server, as described in Section 8.4.5, "Disabling Host Name Verification," if not already disabled.

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 communication between the Administration Server and Node Manager in WCCHOST*n*. If host name verification was already disabled on the source server from which the new one has been cloned, then these steps are not required (the host name verification setting is propagated to the cloned server).

7. Start and test the new Managed Server from the WebLogic Server Administration Console:

    a. Ensure that the newly created Managed Server, WLS_SOA*n*, is running.

    b. Access the application on the LBR (`http://wccinternal.example.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 the Oracle HTTP Server `*_vh.conf` files. 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 address 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 WCCHOST1, which is already running WLS_SOA1, select WCCHOST2. For new Managed Servers on WCCHOST2, which is already running WLS_SOA2, select WCCHOST1.

> **Note:** The appropriate resources must be available to run the Managed Servers concurrently during migration.

    f. Verify that the **Automatic Server Migration Enabled** option is selected.

       This option enables Node Manager to start a failed server on the target node automatically.

    g. Click **Save**.

    h. Restart Node Manager, the Administration Server, and the servers for which server migration has been configured:

       * First, stop the Managed Servers through the Administration Console.

       * Then restart the Node Manager and Administration Server, as described in step 11 under Section 8.4.5, "Disabling Host Name Verification,"

       * Finally, start the Managed Servers again, through the Administration Console.

9. 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*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_SOAn
  ```

- Watch the Node Manager Console for a message indicating that WLS_SOA1's floating IP address has been disabled.

- Wait for Node Manager to attempt a second restart of WLS_SOA*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 WebLogic Server 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.

19.7 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 Oracle Fusion Middleware. (Use the existing installations in shared storage for creating a new Managed Server. You do not need to install WebLogic Server or Oracle 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 WebLogic Server home is shared by multiple servers in different nodes, Oracle recommends that you keep the Oracle Inventory and Middleware home list in those nodes updated for consistency in the installation and application of patches. To update the `oraInventory` directory 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 WebLogic Server 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.

Scale-Out Procedure

The scale-out procedure depends on the topology component:

- Section 19.7.1, "Scale-Out Procedure for WebCenter Content"
- Section 19.7.2, "Scale-Out Procedure for Oracle WebCenter Content: Imaging"
- Section 19.7.3, "Scale-Out Procedure for Oracle WebCenter Enterprise Capture"
- Section 19.7.4, "Scale-Out Procedure for Oracle SOA Suite"

19.7.1 Scale-Out Procedure for WebCenter Content

The scale-out procedure for WebCenter Content adds a WLS_WCC*n* Managed Server configured on a new node.

To scale out the WebCenter Content 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 domain directory, and ensure that the new node has access to this directory, just like the rest of the nodes in the domain.

    > **Note:** These steps are based on the assumption that you are adding a new WebCenter Content server to node *n*, where no Managed Server was running previously.

2. To attach *ORACLE_HOME* in shared storage to the local Oracle Inventory, execute the following commands on WCCHOST*n* (if not already done):

    ```
    cd ORACLE_COMMON_HOME/oui/bin/

    ./attachHome.sh -jreLoc MW_HOME/jrockit_160_version
    ```

> **Note:** The examples documented in this guide use Oracle JRockit. Any certified version of Java can be used for this procedure and is fully supported unless otherwise noted.

To update the Middleware home list, create (or edit, if another WebLogic Server installation exists in the node) the *MW_HOME*/bea/beahomelist file, and add /u01/oracle/products/fmw_home to it.

3. Log in to the WebLogic Server Administration Console.

4. Create a new machine for the new node that will be used, and add the machine to the domain.

> **Note:** If the WLS_WCC*n* server is scaled out on a host where a domain and applications directories already exist, then the '-overwrite_domain option must be specified in the unpack command.

5. Update the machine's Node Manager address to map the IP address 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_WCC*n*, where *n* is a number.

> **Note:** These steps are based on the assumption that you are adding a new server to node *n*, where no Managed Server was running previously.

7. Assign the host name or IP address of WCCHOST*n* to use for the new Managed Server as the **Server Listen Address** of the Managed Server.

8. Assign a WLS_WCC*n* Managed Server to the newly created machine.

   Select a WLS_WCC*n* server from the list of available servers, and click **Finish** and **Activate Changes**.

9. Run the pack command on WCCHOST1 to create a template pack:

> **Note:** You need to do this step and the next two steps because the domain directory for Managed Servers has not yet been created on WCCHOST*n*.

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true -domain=ASERVER_HOME
-template=edgdomaintemplateScaleWCC.jar -template_name=edgdomain_
templateScaleWCC
```

In the reference topology, *ORACLE_COMMON_HOME* is the /u01/oracle/products/fmw_home/oracle_common directory, and *ASERVER_HOME* is the /u01/oracle/config/domains/WCCDomain directory.

10. Run the following command on WCCHOST1 to copy the created template file to WCCHOST*n*:

```
scp edgdomaintemplateScaleWCC.jar oracle@WCCHOSTn:/ORACLE_COMMON_
HOME/common/bin
```

11. Run the `unpack` command on WCCHOST*n* to unpack the template in the Managed Server domain directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh –domain=/u02/oracle/config/domains/WCCDomain
-template=edgdomaintemplateScaleWCC.jar –app_
dir=/u01/oracle/config/applications/WCCDomain
```

12. Run the following commands on WCCHOST*n* to start Node Manager:

```
CD WL_HOME/server/bin
nohup ./startNodeManager.sh > nm.out&
```

In the reference topology, *WL_HOME* is the `/u01/oracle/products/fmw_home/wlserver_10.3` directory.

13. Disable host name verification for the new Managed Server, as described in Section 8.4.5, "Disabling Host Name Verification," if not already disabled.

Before you can start and verify the WLS_WCC*n* Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for communication between the Administration Server and Node Manager in WCCHOST*n*. If host name verification was already disabled on the source server from which the new one has been cloned, then these steps are not required (the host name verification setting is propagated to the cloned server).

14. Start the new Managed Server, WLS_WCC*n*, from the WebLogic Server Administration Console, and verify that the server status is reported as **Running**.

15. Configure the new Managed Server, WLS_WCC*n*:

a. Log in to WLS_WCC*n* at `http://WCCHOSTn:16200/cs` using your 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 name, such as WLS_WCC1.

- **Content Server Instance Folder:** Set this to `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs`.

- **Native File Repository Location:** Set this to `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs/vault`.

- **WebLayout Folder:** Set this to
/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs/weblayout.

- **User Profile:** Set this to /u01/oracle/config/domains/WCCDomain/WCC_
Cluster/cs/data/users/profiles.

   c. Click **Submit** when finished, and restart the new Managed Server, using the
WebLogic Server Administration Console.

16. Add the WLS_WCC*n* listen addresses to the list of allowed hosts in Oracle
WebCenter Content in the file
/u01/oracle/config/domains/WCCDomain/WCC_
Cluster/cs/config/config.cfg. Restart the Oracle WebCenter Content Managed
Servers through the Administration Console.

The servers and listen addresses to be added in the Content Server pool follow:

- `WCCHOST1:4444`

- `WCCHOST2:4444`

- `WCCHOST3:4444`

For more information, see Section 13.5.12, "Creating a Connection to Content
Server."

17. Test the WLS_WCC*n* Managed Server by accessing the application on the LBR
(`https://wcc.example.com/cs`). 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). Its is not required to add all servers in a cluster to the
> WebLogicCluster directive in the Oracle HTTP Server `*_vh.conf` files.
> 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.

19.7.2 Scale-Out Procedure for Oracle WebCenter Content: Imaging

The scale-out procedure for Imaging adds a WLS_IMG*n* Managed Server configured
on a new node.

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 commands on WCCHOST*n* (if not already done):

```
cd ORACLE_COMMON_HOME/oui/bin/
```

```
./attachHome.sh -jreLoc MW_HOME/jrockit_160_version
```

To update the Middleware home list, create (or edit, if another WebLogic Server
installation exists in the node) the `MW_HOME/bea/beahomelist` file, and add `MW_
HOME` to it.

> **Note:** The examples documented in this guide use Oracle JRockit. Any certified version of Java can be used for this procedure and is fully supported unless otherwise noted.

3. Log in to the WebLogic Server Administration Console.

4. Create a new machine for the new node that will be used, and add the machine to the domain.

> **Note:** If the WLS_IMG*n* server is scaled out in the same machine as the WLS_WCC*n* server, then you do not need to create a new machine. Use the same Machine created in Section 19.7.1, "Scale-Out Procedure for WebCenter Content," Step 4.

5. Update the machine's Node Manager address to map the IP address 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_IMG*n*, where *n* is a number.

> **Note:** These steps are based on the assumption that you are adding a new server to node *n*, where no Managed Server was running previously.

   a. Assign the host name or IP address 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 virtual IP address (also called a floating IP address) for the server. This virtual IP address should be different from the one used for the existing Managed Server.

   > **Note:** You must enable a virtual IP address on node *n*, and you must also correctly resolve the host names in the network system used by the topology (with either DNS server or host resolution). For information about how to enable the virtual IP addresses, see Section 6.6, "Enabling Virtual IP Addresses"

   b. Select **Yes, make this server a member of an existing cluster.**

   c. Assign the newly created server to the machine you added in step 4. Without this, the machine name of the cloned server will remain.

7. 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 persistence store for the new IpmJmsServer*N* (which will be created in a later step) and name it, for example, `IMGJMSServer`*N*`Store`. Specify the path for the store as recommended in Section 4.4, "Recommended Locations for Different Directories" as the directory for the JMS persistence stores:

```
/u01/oracle/config/domains/WCCDomain/IMG_Cluster/jms
```

b. Create a new JMS server for; for example, `IpmJmsServer`*N*.

Use the IMGJMSServer*N*Store created previously for this JMS server. Target the IpmJmsServer*N* server to the recently created Managed Server (WLS_ IMG*n*).

8. Run the `pack` command on WCCHOST1 to create a template pack:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true -domain=ASERVER_HOME
-template=edgdomaintemplateScaleIMG.jar
-template_name=edgdomain_templateScaleIMG
```

In the reference topology, *ORACLE_COMMON_HOME* is the `/u01/oracle/products/fmw_ home/oracle_common` directory, and *ASERVER_HOME* is the `/u01/oracle/config/domains/WCCDomain` directory.

> **Note:** If the domain directory for other Managed Servers resides on a shared directory, this step and the next two steps are not required. Instead, the new nodes mount the already existing domain directory and use it for the newly added Managed Server.

9. Run the following command on WCCHOST1 to copy the created template file to WCCHOST*n*:

```
scp edgdomaintemplateScaleIMG.jar oracle@WCCHOSTn:/ORACLE_COMMON_
HOME/common/bin
```

> **Note:** If the new host, WCCHOST*n*, will use the same Middleware home as WCCHOST1, then this step is not required.

10. Run the `unpack` command on WCCHOST*n* to unpack the template in the Managed Server domain directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME -template= edgdomaintemplateScaleIMG.jar -app_
dir=APPLICATION_HOME
```

In the reference topology, *APPLICATION_HOME* is the `/u01/oracle/config/applications/WCCDomain` directory.

> **Note:** If the WLS_IMG*n* server is scaled out on a host where a
> domain and applications directories already exist, then the
> '-overwrite_domain option must be specified in the unpack command.

11. Disable host name verification for the new Managed Server, as described in
    Section 8.4.5, "Disabling Host Name Verification," if not already disabled.

    Before you can start and verify the WLS_WCC*n* Managed Server, you must disable
    host name verification. You can re-enable it after you have configured server
    certificates for communication between the Administration Server and Node
    Manager in WCCHOST*n*. If host name verification was already disabled on the
    source server from which the new one has been cloned, then these steps are not
    required (the host name verification setting is propagated to the cloned server).

12. Disable the Automatic Server Migration Enabled option:

    a. In the **Domain Structure** tree on the left of the WebLogic Server
        Administration Console, expand **Environment**, and select **Servers**

    b. Select the **WLS_IMG*n*** Managed Server, and click the **Migration** tab.

    c. Unselect **Automatic Server Migration Enabled**.

    d. Click **Save & Activate Changes**.

13. Start Node Manager on the new node if not already started. Run the following
    commands on WCCHOST*n* to start Node Manager:

    ```
    CD WL_HOME/server/bin
    nohup ./startNodeManager.sh > nm.out&
    ```

    In the reference topology, *WL_HOME* is the /u01/oracle/products/fmw_
    home/wlserver_10.3 directory.

14. Start the new Managed Server, WLS_IMG*n*, from Fusion Middleware Control 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 13.5.11, "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.

    > **Note:** Make sure that the host names of all Imaging Managed Servers
    > have been added to the SocketHostNameSecurityFilter parameter
    > list in the /u01/oracle/config/domains/WCCDomain/WCC_
    > Cluster/cs/config/config.cfg file.

16. Restart all Oracle WebCenter Content Managed Servers, using the WebLogic
    Server Administration Console.

17. Test the WLS_IMG*n* Managed Server by accessing the application on the LBR
    (https://wcc.example.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). Its is not required to add all servers in a cluster to the WebLogicCluster directive in the Oracle HTTP Server `*_vh.conf` files. 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.

It is assumed that the source server from which the new one has been cloned (here WLS_IMG*n*) already had server migration configured. If this is the case, the following steps are not required because the server migration settings are propagated to the cloned server.

If host-name verification certificates have been set up for Node Manager, then, as a prerequisite, you should perform these steps for the newly created server. For more information, see Section 16.3, "Enabling Host Name Verification Certificates for Node Manager."

> **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. For more information about privilege requirements, see Chapter 17, "Configuring Server Migration for an Enterprise Deployment."

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.

> **Note:** Specify the least-loaded machine as the migration target for the new server. The required capacity planning must be completed so that this node has enough available resources to sustain an additional Managed Server.

f. 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 Node Manager, the Administration Server, and the servers for which server migration has been configured:

          * First, stop the Managed Servers through the Administration Console.

          * Then restart the Node Manager and Administration Server, as described in step 11 under Section 8.4.5, "Disabling Host Name Verification,"

          * Finally, start the Managed Servers again, through the Administration Console.

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_IMG*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_IMGn
  ```

- Watch the Node Manager Console for a message indicating that WLS_IMG*n*'s floating IP address has been disabled.

- Wait for Node Manager to attempt a second restart of WLS_IMG*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 WebLogic Server 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.

19.7.3 Scale-Out Procedure for Oracle WebCenter Enterprise Capture

The scale-out procedure for Imaging adds a WLS_CPT*n* Managed Server configured on a new node.

To scale out the Capture 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 commands on WCCHOST*n* (if not already done):

```
cd ORACLE_COMMON_HOME/oui/bin/

./attachHome.sh -jreLoc MW_HOME/jrockit_160_version
```

To update the Middleware home list, create (or edit, if another WebLogic Server installation exists in the node) the *MW_HOME*/bea/beahomelist file, and add `/u01/oracle/products/fmw_home` to it.

> **Note:** The examples documented in this guide use Oracle JRockit. Any certified version of Java can be used for this procedure and is fully supported unless otherwise noted.

3. Log in to the WebLogic Server Administration Console.

4. Create a new machine for the new node that will be used, and add the machine to the domain, if not already done.

5. Update the machine's Node Manager address to map the IP address of the node that is being used for scale-out.

6. Use the WebLogic Server Administration Console to clone WLS_CPT1 into a new Managed Server. Name it WLS_CPT*n*, where *n* is a number.

   > **Note:** These steps are based on the assumption that you are adding a new server to node *n*, where no Managed Server was running previously.

   a. Assign the host name or IP address 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 virtual IP address (also called a floating IP address) for the server. This virtual IP address should be different from the one used for the existing Managed Server.

   > **Note:** You must enable a virtual IP address on node *n*, and you must also correctly resolve the host names in the network system used by the topology (with either DNS server or host resolution). For information about how to enable the virtual IP addresses, see Section 6.6, "Enabling Virtual IP Addresses"

   b. 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.

7. Create a JMS server for Capture on the new Managed Server:

   a. Use the WebLogic Server Administration Console to first create a new persistence store for the new CaptureJmsServer*N* (which will be created in a later step) and name it, for example, `CPTJMSServerNStore`. Specify the path for the store, recommended in Section 4.4, "Recommended Locations for Different Directories," as the directory for the JMS persistence stores:

   `MSERVER_HOME/`*cluster_name*`/jms`

   b. Create a new JMS server for; for example, `CaptureJmsServerN`. Use the CPTJMSServer*N*Store persistence store created in the preceding step for this JMS server. Target the CaptureJmsServer*N* server to the recently created Managed Server (WLS_CPT*n*).

8. Run the `pack` command on WCCHOST1 to create a template pack:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true -domain=ASERVER_HOME
-template=edgdomaintemplateScaleCPT.jar
-template_name=edgdomain_templateScaleCPT
```

In the reference topology, *ORACLE_COMMON_HOME* is the /u01/oracle/products/fmw_ home/oracle_common directory, and *ASERVER_HOME* is the /u01/oracle/config/domains/WCCDomain directory.

> **Note:** If the domain directory for other Managed Servers resides on a shared directory, this step and the next two steps are not required. Instead, the new nodes mount the already existing domain directory and use it for the newly added Managed Server.

9. Run the following command on WCCHOST1 to copy the created template file to WCCHOST*n*:

```
scp edgdomaintemplateScaleCPT.jar oracle@WCCHOSTn:/ORACLE_COMMON_
HOME/common/bin
```

> **Note:** If the new host, WCCHOST*n*, will use the same *MW_HOME* as WCCHOST1, then this step is not required.

10. Run the `unpack` command on WCCHOST*n* to unpack the template in the Managed Server domain directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME -template= edgdomaintemplateScaleCPT.jar -app_
dir=APPLICATION_HOME
```

> **Note:** If the `unpack` command for the WLS_CPT*n* server runs on a host where a domain and applications directories already exist, then the '-overwrite_domain option must be specified in the `unpack` command.

11. Disable host name verification for the new Managed Server, as described in Section 8.4.5, "Disabling Host Name Verification," if not already disabled.

Before you can start and verify the WLS_WCC*n* Managed Server, you must disable host name verification. You can re-enable it after you have configured server certificates for communication between the Administration Server and Node Manager in WCCHOST*n*. If host name verification was already disabled on the source server from which the new one has been cloned, then these steps are not required (the host name verification setting is propagated to the cloned server).

12. Disable the `Automatic Server Migration Enabled` option:

a. In the **Domain Structure** tree on the left of the WebLogic Server Administration Console, expand **Environment**, and select **Servers**

b. Select the **WLS_CPT*n*** Managed Server, and click the **Migration** tab.

    c. Unselect **Automatic Server Migration Enabled**.

    d. Click **Save & Activate Changes**.

13. Start Node Manager on the new node if not already started. Run the following commands on WCCHOST*n* to start Node Manager:

```
CD WL_HOME/server/bin
nohup ./startNodeManager.sh > nm.out&
```

In the reference topology, *WL_HOME* is the `/u01/oracle/products/fmw_home/wlserver_10.3` directory.

14. Start the new Managed Server, WLS_CPT*n*, from Fusion Middleware Control and make sure it is running.

15. Add the new Capture server listen addresses to the list of allowed hosts in Oracle WebCenter Content Server. Follow the steps in Section 13.5.11, "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.

> **Note:** Make sure that the host names of all Capture Managed Servers have been added to the `SocketHostNameSecurityFilter` parameter list in the `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs/config/config.cfg` file.

16. Restart all Oracle WebCenter Content Managed Servers, using the WebLogic Server Administration Console.

17. Test the WLS_CPT*n* Managed Server by accessing the application on the LBR (`https://wcc.example.com/dc-console` for the Capture console, and `https://wcc.example.com/dc-client` for the Capture client). 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). Its is not required to add all servers in a cluster to the WebLogicCluster directive in the Oracle HTTP Server `*_vh.conf` files. 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.

It is assumed that the source server from which the new one has been cloned (here WLS_CPT*n*) already had server migration configured. If this is the case, the following steps are not required because the server migration settings are propagated to the cloned server.

If host-name verification certificates have been set up for Node Manager, then, as a prerequisite, you should perform these steps for the newly created server. For more information, see Section 16.3, "Enabling Host Name Verification Certificates for Node Manager."

> **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. For more information about privilege requirements, see Chapter 17, "Configuring Server Migration for an Enterprise Deployment."

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.

> **Note:** Specify the least-loaded machine as the migration target for the new server. The required capacity planning must be completed so that this node has enough available resources to sustain an additional Managed Server.

f. 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 Node Manager, the Administration Server, and the servers for which server migration has been configured:

  * First, stop the Managed Servers through the Administration Console.

  * Then restart the Node Manager and Administration Server, as described in step 11 under Section 8.4.5, "Disabling Host Name Verification,"

  * Finally, start the Managed Servers again, through the Administration Console.

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_CPT*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_CPTn
    ```

  ■ Watch the Node Manager Console for a message indicating that WLS_CPT*n*'s floating IP address has been disabled.

- Wait for Node Manager to attempt a second restart of WLS_CPT*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 WebLogic Server 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.

19.7.4 Scale-Out Procedure for Oracle SOA Suite

The scale-out procedure for Imaging adds a WLS_SOA*n* Managed Server configured on a new node.

> **Note:** To scale out the Oracle SOA Suite subsystem used by Capture, refer to the Oracle SOA Suite enterprise deployment topology documentation.

To scale out the Oracle SOA Suite servers in the enterprise deployment topology:

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, run the following commands on WCCHOST*n* (if not already done):

   ```
   cd ORACLE_COMMON_HOME/oui/bin/
   ```

   ```
   ./attachHome.sh –jreLoc MW_HOME/jrockit_160_version
   ```

   To update the Middleware home list, create (or edit, if another WebLogic Server installation exists in the node) the `MW_HOME`/bea/beahomelist file, and add `/u01/oracle/products/fmw_home` to it.

   > **Note:** The examples documented in this guide use Oracle JRockit. Any certified version of Java can be used for this procedure and is fully supported unless otherwise noted.

3. Log in to the WebLogic Server Administration Console.

4. Create a new machine for the new node that will be used, and add the machine to the domain.

   > **Note:** If the WLS_SOA*n* server is scaled out on a host where a domain and applications directories already exist, then the `'–overwrite_domain` option must be specified in the `unpack` command.

5. Update the machine's Node Manager address to map the IP address 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 are based on the assumption that you are adding a new server to node *n*, where no Managed Server was running previously.

7. Assign the host name or IP address 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 virtual IP address (also called a floating IP address) for the server. This virtual IP address should be different from the one used for the existing Managed Server.

8. Run the `pack` command on WCCHOST1 to create a template pack:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh –managed=true –domain=ASERVER_HOME
–template=edgdomaintemplateScaleSOA.jar
–template_name=edgdomain_templateScaleSOA
```

> **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.

9. Run the following command on WCCHOST1 to copy the created template file to WCCHOST2:

```
scp edgdomaintemplateScaleSOA.jar oracle@WCCHOST2:/ORACLE_COMMON_
HOME/common/bin
```

10. Run the `unpack` command on WCCHOST2 to unpack the template in the Managed Server domain directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh –domain=MSERVER_HOME –template= edgdomaintemplateScaleSOA.jar
–app_dir=APPLICATION_HOME
```

> **Note:** If the WLS_CPT*n* server is scaled out on a host where a domain and applications directories already exist, then the '`-overwrite_domain` option must be specified in the `unpack` command.

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 persistence 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 4.4, "Recommended Locations for Different Directories":

   ```
   /u01/oracle/config/domains/WCCDomain/SOA_Cluster/jms
   ```

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 UMSJMSServer (for example, `UMSJMSFileStore_N`). Specify the path for the store. This should be a directory on shared storage, as recommended in Section 4.4, "Recommended Locations for Different Directories":

`/u01/oracle/config/domains/WCCDomain/SOA_Cluster/jms`

> **Note:** You can also assign `SOAJMSFileStore_N` as the store for the new UMS JMS servers. For the purpose of clarity and isolation, individual persistence stores are used in the following steps.

d. Create a new JMS server for UMS (for example, `UMSJMSServer_N`). Use `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 **Domain Structure** tree on the left of the WebLogic Server Administration Console, and then expand the **Messaging** node. Click **JMS Modules**. The JMS Modules page opens. Click **SOAJMSModule** (represented as a hyperlink in the **Names** column of the table). The Settings page for SOAJMSModule opens. Open the **SubDeployments** tab, which shows information about the subdeployment module for SOAJMS.

> **Note:** This subdeployment module name is a random name in the form of `SOAJMSServer`*XXXXXX* resulting from the Configuration Wizard JMS configuration for the first two servers (WLS_SOA1 and WLS_ SOA2).

Click the **SOAJMSServer***XXXXXX* 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 **Domain Structure** tree on the left of the WebLogic Server Administration Console, and then expand the **Messaging** node. Click **JMS Modules**. The JMS Modules page opens. Click **UMSJMSSystemResource** (represented as a hyperlink in the Names column of the table). The Settings page for UMSJMSSystemResource opens. Open the **SubDeployments** tab, which shows information about the subdeployment module for UMSJMS.

> **Note:** This subdeployment module name is a random name in the form of `UCMJMSServer`*XXXXXX* resulting from the Configuration Wizard JMS configuration for the first two servers (WLS_SOA1 and WLS_ SOA2).

Click the **UMSJMSServer***XXXXXX* subdeployment. Add the new JMS server for UMS called UMSJMSServer_N to this subdeployment. Click **Save**.

12. Configure a Tx persistence store for the new server. This should be a location visible from other nodes as indicated in the recommendations about shared storage (see Section 4.4, "Recommended Locations for 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 persistence store to store its data files:

   ```
   /u01/oracle/config/domains/WCCDomain/SOA_Cluster/tlogs
   ```

13. Disable host name verification for the new Managed Server, as described in Section 8.4.5, "Disabling Host Name Verification," if not already disabled.

   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 communication between the Administration Server and Node Manager in WCCHOST*n*. If host name verification was already disabled on the source server from which the new one has been cloned, then these steps are not required (the host name verification setting is propagated to the cloned server).

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 WCCHOST*n*):

   ```
   cd WL_HOME/server/bin
   nohup ./startNodeManager.sh > nm.out& New_Node_IP
   ```

   In the reference topology, *WL_HOME* is the /u01/oracle/products/fmw_home/wlserver_10.3 directory.

15. Start the new Managed Server, WLS_SOA*n*, from the WebLogic Server Administration Console, and make sure it is running.

16. Test the WLS_SOA*n* Managed Server by accessing the application on the LBR (http://wccinternal.example.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). Its is not required to add all servers in a cluster to the WebLogicCluster directive in the Oracle HTTP Server *_vh.conf files. 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 address 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 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.

> **Note:** Specify the least-loaded machine as the migration target for the new server. The required capacity planning must be completed so that this node has enough available resources to sustain an additional Managed Server.

f. 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 Node Manager, the Administration Server, and the servers for which server migration has been configured:

  * First, stop the Managed Servers through the Administration Console.

  * Then restart the Node Manager and Administration Server, as described in step 11 under Section 8.4.5, "Disabling Host Name Verification,"

  * Finally, start the Managed Servers again, through the Administration Console.

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*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_SOAn
    ```

  ■ Watch the Node Manager Console for a message indicating that WLS_SOA*n*'s floating IP address has been disabled.

  ■ Wait for Node Manager to attempt a second restart of WLS_SOA*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 WebLogic Server 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.

19.8 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 WCCHOST1 to WCCHOST2:

- Section 19.8.1, "Assumptions and Procedure"

- Section 19.8.2, "Validating Access to WCCHOST2 Through the Load Balancer"

- Section 19.8.3, "Failing the Administration Server Back to WCCHOST1"

19.8.1 Assumptions and Procedure

Note the following assumptions:

- The Administration Server is configured to listen on ADMINVHN, and not on *any* address. See step 16 in Section 8.3, "Running the Configuration Wizard on WCCHOST1 to Create a Domain."

- The Administration Server is failed over from WCCHOST1 to WCCHOST2, and the two nodes have these IP addresses:

  - WCCHOST1: 100.200.140.165

  - WCCHOST2: 100.200.140.205

  - ADMINVHN: 100.200.140.206. This is the virtual IP address where the Administration Server is running, assigned to eth*X*:*Y*.

- The domain directory where the Administration Server is running in WCCHOST1 is on a shared storage and is mounted also from WCCHOST2.

- Oracle WebLogic Server and Oracle Fusion Middleware components have been installed on WCCHOST2 as described in Chapter 7, "Installing the Software for an Enterprise Deployment" (that is, the same paths for *ORACLE_HOME* and *MW_HOME* that exist on WCCHOST1 are also available on WCCHOST2).

To fail over the Administration Server to a different node (WCCHOST2):

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 WCCHOST1 (where *X:Y* is the current interface used by ADMINVHN):

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

   b. Run the following command on WCCHOST2:

   ```
   /sbin/ifconfig interface:index IP_address netmask netmask
   ```

   For example:

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

   Note: Make sure that the netmask and interface to be used match the available network configuration in WCCHOST2. Also, make sure that the location of the Administration Server application directory is mounted as described in Section 4.4, "Recommended Locations for Different Directories."

   ---

    c. Update the routing tables on WCCHOST2 using `arping`; for example:

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

3. Start Node Manager on WCCHOST2, as described in Section 8.4.2, "Starting Node Manager on WCCHOST1."

4. Start the Administration Server on WCCHOST2, as described in Section 8.4.3, "Starting the Administration Server on WCCHOST1."

5. Test that you can access the Administration Server on WCCHOST2 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`.

19.8.2 Validating Access to WCCHOST2 Through the Load Balancer

Perform the same steps as in Section 9.6.4, "Validating Access Through the Load Balancer." This is to check that you can access the Administration Server when it is running on WCCHOST2.

19.8.3 Failing the Administration Server Back to WCCHOST1

This step checks that you can fail back the Administration Server; that is, stop it on WCCHOST2 and run it on WCCHOST1 again.

To migrate ADMINVHN back to the WCCHOST1 node:

1. Make sure the Administration Server is not running.

2. Run the following command on WCCHOST2.

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

3. Run the following command on WCCHOST1:

```
/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 WCCHOST1.

4. Update the routing tables using `arping`. Run the following command from WCCHOST1:

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

5. Start the Administration Server again on WCCHOST1, as described in Section 8.4.3, "Starting the Administration Server on WCCHOST1."

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`.

19.9 Performing Backups and Recoveries in Oracle WebCenter Content Enterprise Deployments

Table 19–2 lists the static artifacts to back up in the Oracle WebCenter Content 11*g* enterprise deployment.

Table 19–2   Static Artifacts to Back Up in the Oracle WebCenter Content 11g Enterprise Deployment

Type	Host	Location	Tier
Oracle home (DB)	WCCDBHOST1 and WCCDBHOST2	The location is user defined.	Data tier
Middleware home (OHS)	WEBHOST1 and WEBHOST2	`/u02/oracle/products/fmw_home/web_home`	Web tier
Middleware home (`MW_HOME`, which includes the Oracle WebCenter Content and Oracle SOA Suite Oracle homes)	WCCHOST1 and WCCHOST2*	`/u01/oracle/products/fmw_home` The Oracle WebCenter Content and Oracle SOA Suite Oracle homes are also under `MW_HOME`:	Application tier
Installation-related files		`OraInventory`, `User_Home`/bea/beahomelist, `oraInst.loc`, `oratab`	N/A

Table 19–3 lists the runtime artifacts to back up in the Oracle WebCenter Content 11*g* enterprise deployment.

Table 19–3   Runtime Artifacts to Back Up in the Oracle WebCenter Content 11g Enterprise Deployment

Type	Host	Location	Tier
Application artifacts (EAR and WAR files)	WCCHOST1 and WCCHOST2	Find the application artifacts by viewing all of the deployments through the administration console.	Application tier
Oracle WebCenter Content runtime artifacts	WCCHOST1 or WCCHOST2	`/u01/oracle/config/domains/WCCDomain/WCC_Cluster`	Application tier
Capture runtime artifacts	WCCHOST1 or WCCHOST2	`/u01/oracle/config/domains/WCCDomain/CPT_Cluster`	Application tier
Oracle WebCenter Enterprise Capture runtime artifacts	WCCHOST1 or WCCHOST2	`/u01/oracle/config/domains/WCCDomain/CPT_Cluster`	Application tier
Oracle SOA Suite runtime artifacts	WCCHOST1 or WCCHOST2	`/u01/oracle/config/domains/WCCDomain/SOA_Cluster`	Application tier

Customized Managed Server configuration for Oracle WebCenter Content	WCCHOST1 or WCCHOST2	`/u02/oracle/config/domains/WCCDomain/ucm/cs/bin/intradoc.cfg`
		
		and
		
		`/u02/oracle/config/domains/WCCDomain/bin/server_migration/wlsifconfig.sh`
			Application tier

Table 19–3   (Cont.) Runtime Artifacts to Back Up in the Oracle WebCenter Content 11g Enterprise

Type	Host	Location	Tier
Customized Managed Server configuration for Oracle SOA Suite	WCCHOST1 or WCCHOST2	If using UMS: `/u02/oracle/config/domains/WCCDomain/servers/server_name/tmp/_WL_user/ums_driver_name/*/configuration/driverconfig.xml` (where `*` represents a directory whose name is randomly generated by WebLogic Server during deployment; for example, `3682yq`) and `/u02/oracle/config/domains/WCCDomain/bin/server_migration/wlsifconfig.sh`	Application tier
Oracle HTTP Server instance home	WEBHOST1 and WEBHOST2	/u02/oracle/config/web*N*	Web tier
Oracle RAC databases	WCCDBHOST1 and WCCDBHOST2	The location is user-defined.	Data tier

For more information on backup and recovery of Oracle Fusion Middleware components, see the *Oracle Fusion Middleware Administrator's Guide*.

19.10 Maintaining an OPSS Security Store in Oracle Database

This section describes a few tasks that an administrator can follow to maintain a security store in Oracle Database.

A database-based security store maintains a change log that should be periodically purged. To purge it, an administrator can use the provided SQL script `opss_purge_changelog.sql`, which will purge change logs older than 24 hours, or connect to the database and run SQL `delete` (with the appropriate arguments) as illustrated in the following lines:

```
SQL>delete from jps_changelog where createdate < (select(max(createdate) - 1) from
jps_changelog);
SQL>Commit;
```

If the OPSS management API performs slowly while accessing the database-based security store, run the `DBMS_STATS` package to gather statistics about the physical storage of a DB table, index, of cluster. This information is stored in the data dictionary and can be used to optimize the execution plan for SQL statements accessing analyzed objects.

When loading large amount of data into a database-based security store, such as when creating thousands of new application roles, it is recommended that `DBMS_STATS` be run within short periods and concurrently with the loading activity. Otherwise, when the loading activity is small, `DBMS_STATS` needs to be run just once and according to your needs.

The following sample illustrates the use of `DBMS_STATS`:

```
EXEC DBMS_STATS.GATHER_SCHEMA_STATS('WCC_OPSS', DBMS_STATS.AUTO_SAMPLE_SIZE, no_
invalidate=>FALSE);
```

where `WCC_OPSS` denotes the name of the DB schema created during the RCU setup (see Section 5.4, "Creating Database Schemas"). For details about the `DBMS_STATS` package, see the *Oracle Database Administrator's Guide*.

To run `DBMS_STATS` periodically, use a shell script or an SQL script, as described next.

The following sample script runs the command `DBMS_STATS` every 10 minutes:

```
#!/bin/sh
i=1
while [ $i -le 1000 ]
do
echo $i
sqlplus wcc_opss/welcome1@inst1 @opssstats.sql
sleep 600
i=`expr $i + 1`
done
```

where `opssstats.sql` contains the following text:

```
EXEC DBMS_STATS.gather_schema_stats('WCC_OPSS',DBMS_STATS.AUTO_SAMPLE_SIZE, no_
invalidate=>FALSE);
QUIT;
```

The following sample SQL script also runs the command `DBMS_STATS` every 10 minutes:

```
variable jobno number;
BEGIN
DBMS_JOB.submit
(job => :jobno,
what => 'DBMS_STATS.gather_schema_stats(''WCC_OPSS'',DBMS_STATS.AUTO_SAMPLE_
SIZE,no_invalidate=>FALSE);',
interval => 'SYSDATE+(10/24/60)');
COMMIT;
END;
/
```

To stop the periodic invocation of `DBMS_STATS` by the above SQL script, first find out its job number by issuing the following commands:

```
sqlplus '/as sysdba'
SELECT job FROM dba_jobs WHERE schema_user = 'WCC_OPSS' AND what = 'DBMS_
STATS.gather_schema_stats(''WCC_OPSS'',DBMS_STATS.AUTO_SAMPLE_SIZE, no_
invalidate=>FALSE);';
```

Then issue a command like the following, in which it is assumed that the query above returned the job number 31:

```
EXEC DBMS_JOB.remove(31);
```

19.11 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 virtual IP addresses 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.

19.12 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 *Oracle Fusion Middleware Developing Oracle WebCenter Content: Imaging* and *Installing and Configuring Oracle WebCenter Content*.

19.13 Troubleshooting the Oracle WebCenter Content Enterprise Deployment Topology

This section covers the following topics:

- Section 19.13.1, "Page Not Found When Accessing soa-infra Application Through Load Balancer"

- Section 19.13.2, "Soa-infra Application Fails to Start Due to Deployment Framework Issues (Coherence)"

- Section 19.13.3, "WebCenter Content, Oracle SOA Suite, or Imaging Server Fails to Start Due to Maximum Number of Processes Available in Database"

- Section 19.13.4, "Administration Server Fails to Start After a Manual Failover"

- Section 19.13.5, "Error While Activating Changes in Administration Console"

- Section 19.13.6, "SOA, Imaging, or Capture Server Not Failed Over After Server Migration"

- Section 19.13.7, "SOA, Imaging, or Capture Server Not Reachable from Browser After Server Migration"

- Section 19.13.8, "OAM Configuration Tool Does Not Remove URLs"

- Section 19.13.9, "Redirection of Users to Login Screen After Activating Changes in the Administration Console"

- Section 19.13.10, "Redirection of Users to Administration Console's Home Page After Activating Changes to Oracle Access Manager"

- Section 19.13.11, "Configured JOC Port Already in Use"

- Section 19.13.12, "Using CredentialAccessPermissions to Allow Oracle WebCenter Content: Imaging to Read Credentials from the Credential Store"

- Section 19.13.13, "Improving Performance with Very Intensive Document Uploads from Oracle WebCenter Content: Imaging to Oracle WebCenter Content"

- Section 19.13.14, "Out-of-Memory Issues on Managed Servers"

- Section 19.13.15, "Regenerating the Master Password for Oracle WebCenter Content Managed Servers"

- Section 19.13.16, "Logging Out from the WebLogic Server Administration Console Does Not End the User Session"

- Section 19.13.17, "Transaction Timeout Error"

- Section 19.13.18, "Caching and Locking Files"
- Section 19.13.19, "Modifying Upload and Stage Directories for Applications Deployed Remotely"

19.13.1 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.

19.13.2 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 runtime 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 the *Oracle Coherence Developer's Guide*.

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 one are reported in the server's output log if any of the addresses is not resolved correctly:

```
oracle.integration.platform.blocks.deploy.CompositeDeploymentCoordinatorMessage
s errorUnableToStartCoherence
```

19.13.3 WebCenter Content, Oracle SOA Suite, or Imaging Server Fails to Start Due to Maximum Number of Processes Available in Database

Problem: A WebCenter Content, Oracle SOA Suite, or Imaging server fails to start. The domain has been extended for new a type of Managed Server (for example, WebCenter Content extended for Imaging) or the system has been scaled up (added new servers of the same type). The WebCenter Content, Oracle SOA Suite, or Imaging server output log reports the following exception:

```
<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. For information about parameter files, server parameter files, and how to change parameter value, see the *Oracle Database Administrator's Guide*.

19.13.4 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: ASERVER_
HOME/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 *ASERVER_HOME*/servers/AdminServer/data/ldap/ldapfiles/EmbeddedLDAP.lok.

19.13.5 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.

19.13.6 SOA, Imaging, or Capture Server Not Failed Over After Server Migration

Problem: After the maximum restart attempts by the local Node Manager has been reached, Node Manager in the failover node tries to restart the server, but the it does not come up. The server seems to be failed over as reported by Node Manager's output information. The virtual IP address used by the Oracle SOA Suite, Oracle WebCenter Content: Imaging, or Oracle WebCenter Enterprise Capture server is not enabled in the failover node after Node Manager tries to migrate it (`ifconfig` in the failover node does not report the virtual IP address in any interface). Executing the command `sudo ifconfig $INTERFACE $ADDRESS $NETMASK` does not enable the IP address 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.

19.13.7 SOA, Imaging, or Capture 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*:7001/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 virtual IP address has been migrated and the server started. The virtual IP address used by the Oracle SOA Suite, Imaging, or Capture 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 Mnager 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 address is enabled and *ADDRESS* is the virtual IP address.

19.13.8 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 Oracle Access Manager. Log in to the Access Administration site for Oracle Access Manager, click **My Policy Domains**, click the created policy domain (**SOA_EDG**), then click the **Resources** tab, and remove the incorrect URLs.

19.13.9 Redirection of Users to Login Screen After Activating Changes in the Administration Console

Problem: After configuring OHS and LBR to access the WebLogic Server 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.example.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.

19.13.10 Redirection of Users to Administration Console's Home Page After Activating Changes to Oracle Access Manager

Problem: After configuring Oracle Access Manager, 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 Oracle Access Manager 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** and then **Shared Preferences**, and unselect the **Follow Configuration Changes** checkbox.

19.13.11 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.

19.13.12 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 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 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:

```
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.

19.13.13 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 for 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 `/u01/oracle/config/domains/WCCDomain/WCC_Cluster/cs/config/config.cfg` in a text editor.

2. Remove or comment out the following lines:

   ```
   SocketHostNameSecurityFilter=localhost|localhost.example.com|wcchost1vhn1|wccho
   st2vhn1
   AlwaysReverseLookupForHost=Yes
   ```

3. Add the IP addresses (listen addresses) of the WLS_CPT1 and WLS_CPT2
   Managed Servers (WCCHOST1VHN3 and WCCHOST2VHN3, 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
   ```

   In this example, *X.X.X.X* and *Y.Y.Y.Y* are the listen addresses of WLS_CPT1 and
   WLS_CPT2, respectively. (The address 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, using the WebLogic Server Administration
   Console.

19.13.14 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.

To increase the size of the memory heap allocated for the Java VM:

1. Log in to the WebLogic Server 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:** The memory parameter requirements may differ between
   > various JVMs (Sun JDK, Oracle JRockit, or others). For more
   > information, see "Increasing the Java VM Heap Size for Managed
   > Servers" in *Installing and Configuring Oracle WebCenter Content*.

7. Save the configuration changes.

8. Restart all running Managed Servers, using the WebLogic Server Administration
   Console.

19.13.15 Regenerating the Master Password for Oracle WebCenter Content Managed Servers

If 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 *ASERVER_HOME*/config/fmwconfig directory, you can
regenerate the file.

To regenerate the master password for Oracle WebCenter Content Managed Servers:

1. Stop all Oracle WebCenter Content Managed Servers (WLS_WCC*x*).

2. Remove the `cwallet.sso` file from *MSERVER_HOME*/config/fmwconfig/.

3. Remove the `password.hda` file from *ASERVER_HOME*/`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 *MSERVER_ HOME*/`config/fmwconfig/` as well as the creation of the `password.hda` file in *ASERVER_HOME*/`wcc_cluster_name`/`cs/config/private/`.

6. Use the Oracle WebCenter Content 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 the *MSERVER_HOME*/`config/fmwconfig` directory to the Administration Server's domain directory at *ASERVER_ HOME*/`config/fmwconfig`.

9. Start the second Oracle WebCenter Content Managed Server, and verify that the Administration Server pushes the updated `cwallet.sso` file to the *MSERVER_ HOME*/`config/fmwconfig` directory 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.

19.13.16 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 Oracle Access Manager 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.

19.13.17 Transaction Timeout Error

Problem: The following transaction timeout error appears in the log:

```
Internal Exception: java.sql.SQLException: Unexpected exception while enlisting
 XAConnection java.sql.SQLException: XA error: XAResource.XAER_NOTA start()
failed on resource 'SOADataSource_soaedg_domain': XAER_NOTA : The XID
is not valid
```

Solution: Check your transaction timeout settings, and be sure that the JTA transaction timeout is less than the DataSource XA Transaction Timeout, which is less than the `distributed_lock_timeout` (at the database).

With the out-of-the-box configuration, the SOA data sources do not set XA timeout to any value. The `Set XA Transaction Timeout` configuration parameter is unchecked in the WebLogic Server Administration Console. In this case, the data sources use the domain-level JTA timeout, which is set to `30`. Also, the default `distributed_lock_ timeout` value for the database is `60`. As a result, the SOA configuration works correctly for any system where transactions are expected to have lower life expectancy than such values. Adjust these values according to the transaction times your specific operations are expected to take.

19.13.18 Caching and Locking Files

Oracle WebCenter Content uses its own locking mechanism for files, so it needs to have access to those files without file-attribute caching and without locking being done by the cluster nodes. If one of the nodes accesses a certain status file and it happens to be cached, that node might attempt to run a process that another node is already working on. Or if a particular file is locked by one of the node clients, this could interfere with access by another node. Unfortunately, disabling file-attribute caching on the file share can impact performance. So it is important to disable caching and locking only on the particular folders that require it. For instance, if you are creating the share through Network File System (NFS), use `noac` and `nolock` for the mount options.

19.13.19 Modifying Upload and Stage Directories for Applications Deployed Remotely

If you are deploying applications remotely, you might need to update your `upload` and `stage` directories to absolute paths after you create the domain and unpack to the `mserver` directory. Absolute path names can prevent issues for remote deployments and confusion for deployments that use the stage mode.

The default path names for these directories follow:

```
./servers/AdminServer/upload
```

```
./servers/server_name/stage
```

A

Using Multi Data Sources with Oracle RAC

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 includes the following sections:

- Section A.1, "About Multi Data Sources and Oracle RAC"
- Section A.2, "Typical Procedure for Configuring Multi Data Sources for an Enterprise Deployment 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 *Oracle Fusion Middleware Configuring and Managing JDBC Data Sources for Oracle WebLogic Server*.

A.2 Typical Procedure for Configuring Multi Data Sources for an Enterprise Deployment 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 procedure.

To configure Multi Data Sources for an enterprise deployment topology:

1. On 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 same schema prefix the data source had when you ran the Repository Creation Utility.

d. Click **Next**.

2. The Configure RAC Multi Data Sources Component Schema screen opens (Figure A–1).

Figure A–1   Configure RAC Multi Data Source Component Schema Screen
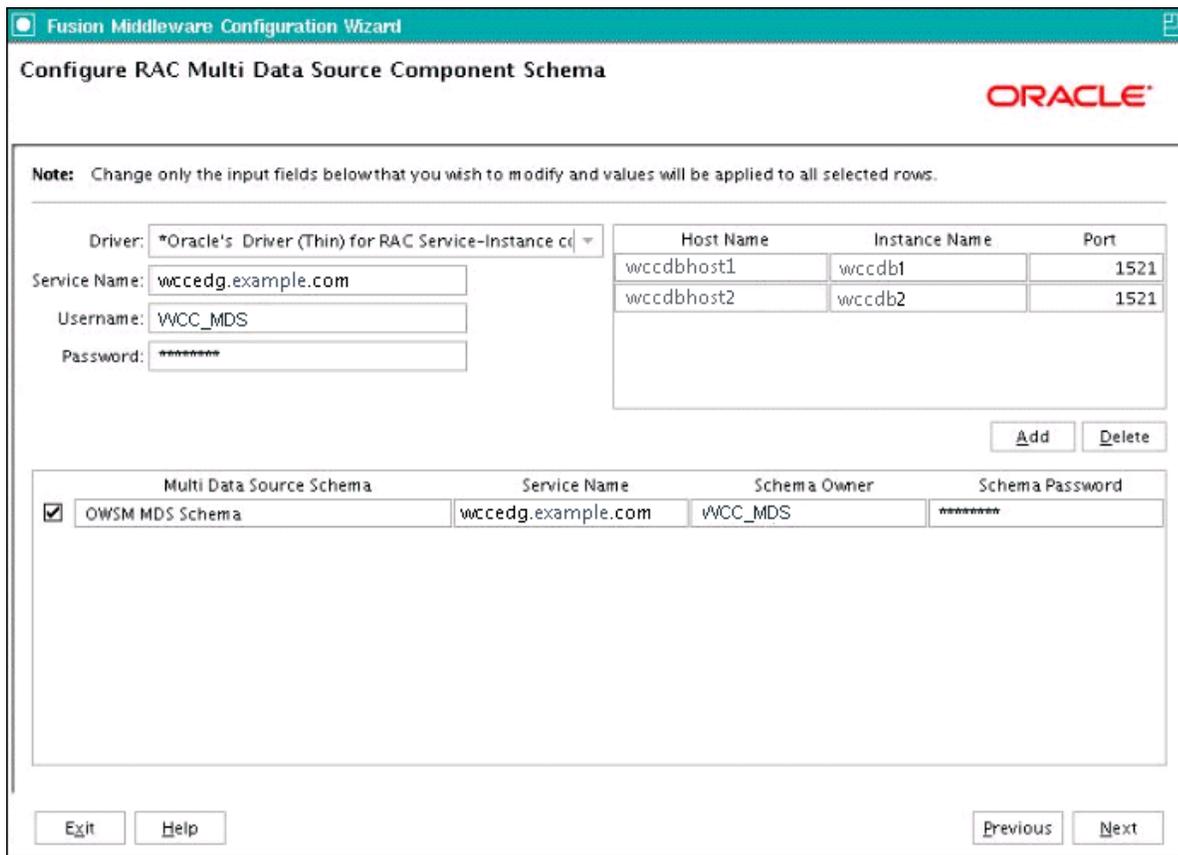
On this screen, perform the following steps:

a. Enter values for the following fields, specifying the connect information for the Oracle RAC database that was seeded with RCU.

  – **Driver:** Select **Oracle's 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 WCC 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. On 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.

B

Targeting Applications and Resources to Servers

This appendix lists the applications, data sources, persistence stores, Java Messaging Service (JMS) modules, and startup and shutdown classes that are targeted to the servers in the Oracle WebLogic Server domain for Oracle WebCenter Content.

This appendix includes the following sections:

- Section B.1, "Applications and Resources for the WebCenter Content Managed Servers"

- Section B.2, "Applications and Resources for the Inbound Refinery Managed Servers"

- Section B.3, "Applications and Resources for the Oracle SOA Suite Managed Servers"

- Section B.4, "Applications and Resources for the Imaging Managed Servers"

- Section B.5, "Applications and Resources for the Capture Managed Servers"

- Section B.6, "Applications and Resources for the Administration Server"

B.1 Applications and Resources for the WebCenter Content Managed Servers

The following applications and resources are targeted to the Oracle WebCenter Content cluster, WCC_Cluster, which includes these Managed Servers:

- WLS_WCC1 on WCCHOST1

- WLS_WCC2 on WCCHOST2

Applications for WebCenter Content

- DMS Application (11.1.1.1.0)

- Oracle UCM Help

- Oracle UCM Native Web Service

- Oracle UCM Web Services

- Oracle WebCenter Content - Content Server

- wsil-wls

Data Sources for WebCenter Content

- `opss-audit-viewDS`

- `opss-audit-DBDS`

- `opss-DBDS`

- `CSDS`

- `leasing`

Startup and Shutdown Classes for WebCenter Content

- `oracle.jrf.AppContextStartup`

- `oracle.dms.wls.DMSStartup`

- `oracle.dms.wls.DMSShutdown`

- `oracle.as.jmx.framework.wls.spi.StartupListener`

- `oracle.ias.cache.Shutdown`

- `oracle.ias.cache.Startup`

- `oracle.security.jps.wls.JpsWlsStartupClass`

- `oracle.jrf.wls.JRFStartup`

- `oracle.core.ojdl.weblogic.ODLConfiguration`

- `oracle.j2ee.ws.server.WebServiceServerStartup`

B.2 Applications and Resources for the Inbound Refinery Managed Servers

The following applications and resources are targeted to the Oracle WebCenter Content: Inbound Refinery servers, IBR_Servers, which include these Managed Servers:

- WLS_IBR1 on WCCHOST1

- WLS_IBR2 on WCCHOST2

Applications for Inbound Refinery

- DMS Application (11.1.1.1.0)

- Oracle UCM Help

- Oracle UCM Native Web Services

- Oracle UCM Web Services

- Oracle WebCenter Content - Inbound Refinery

- wsil-wls

Data Sources for Inbound Refinery

- `opss-audit-viewDS`

- `opss-audit-DBDS`

- `opss-DBDS`

Startup and Shutdown Classes for Inbound Refinery

- `oracle.jrf.AppContextStartup`

- `oracle.dms.wls.DMSStartup`

- `oracle.dms.wls.DMSShutdown`

- `oracle.as.jmx.framework.wls.spi.StartupListener`

- `oracle.ias.cache.Shutdown`

- `oracle.ias.cache.Startup`

- `oracle.security.jps.wls.JpsWlsStartupClass`

- `oracle.jrf.wls.JRFStartup`

- `oracle.core.ojdl.weblogic.ODLConfiguration`

- `oracle.j2ee.ws.server.WebServiceServerStartup`

B.3 Applications and Resources for the Oracle SOA Suite Managed Servers

The following applications and resources are targeted to the Oracle SOA Suite cluster, SOA_Cluster, which includes these Managed Servers:

- WLS_SOA1 on WCCHOST1

- WLS_SOA2 on WCCHOST2

Applications for Oracle SOA Suite

- AqAdapter

- b2bu

- composer

- DbAdapter

- DefaultToDoTaskFlow

- DMS Application (11.1.1.1.0)

- FileAdapter

- FtpAdapter

- JmsAdapter

- MQSeriesAdapter

- OracleAppsAdapter

- OracleBamAdapter

- soa-infra

- SocketAdapter

- usermessagingdriver-email

- usermessagingserver

- worklistapp

- wsil-wls

- wsm-pm

Data Sources for Oracle SOA Suite

- EDNDataSource

- EDNLocalTxDataSource

- mds-owsm

- mds-soa

- opss-audit-viewDS

- opss-audit-DBDS

- opss-DBDS

- OraSDPMDataSource

- SOADataSource

- SOALocalTxDataSource

Persistence Stores for Oracle SOA Suite

- BPMJMSFileStore_auto_1

- BPMJMSFileStore_auto_2

- SOAJMSFileStore_auto_1

- SOAJMSServer_auto_2

- UMSJMSFileStore_auto_1

- UMSJMSFileStore_auto_2

JMS Deployment Modules for Oracle SOA Suite

- BPMJMSServer_auto_1

- BPMJMSServer_auto_2

- SOAJMSServer_auto_1

- SOAJMSServer_auto_2

- UMSJMSServer_auto_1

- UMSJMSServer_auto_2

Startup and Shutdown Classes for Oracle SOA Suite

- oracle.jrf.AppContextStartup

- oracle.dms.wls.DMSStartup

- oracle.dms.wls.DMSShutdown

- oracle.as.jmx.framework.wls.spi.StartupListener

- oracle.ias.cache.Shutdown

- oracle.ias.cache.Startup

- oracle.security.jps.wls.JpsWlsStartupClass

- oracle.jrf.wls.JRFStartup

- `oracle.core.ojdl.weblogic.ODLConfiguration`

- `oracle.bpel.services.common.util.GenerateBPMCryptoKey`

- `oracle.j2ee.ws.server.WebServiceServerStartup`

B.4 Applications and Resources for the Imaging Managed Servers

The following applications and resources are targeted to the Oracle WebCenter Content: Imaging cluster, IMG_Cluster, which includes these Managed Servers:

- WLS_IMG1 on WCCHOST1

- WLS_IMG2 on WCCHOST2

Applications for Imaging

- DMS Application (11.1.1.1.0)

- imaging

- imaging-vc

- wsil-wls

Data Sources for Imaging

- `IPMDS`

- `mds-owsm`

- `opss-audit-viewDS`

- `opss-audit-DBDS`

- `opss-DBDS`

Persistence Stores for Imaging

- `IMGJMSServer1Store`

- `IMGJMSServer2Store`

JMS Deployment Modules for Imaging

- `IpmJmsServer1`

- `IpmJmsServer2`

- `ViewerJmsServer1`

- `ViewerJmsServer3`

Startup and Shutdown Classes for Imaging

- `oracle.jrf.AppContextStartup`

- `oracle.dms.wls.DMSStartup`

- `oracle.dms.wls.DMSShutdown`

- `oracle.as.jmx.framework.wls.spi.StartupListener`

- `oracle.ias.cache.Shutdown`

- `oracle.ias.cache.Startup`

- `oracle.security.jps.wls.JpsWlsStartupClass`

- `oracle.jrf.wls.JRFStartup`

- `oracle.core.ojdl.weblogic.ODLConfiguration`

- `oracle.j2ee.ws.server.WebServiceServerStartup`

B.5 Applications and Resources for the Capture Managed Servers

The following applications and resources are targeted to the Oracle WebCenter Enterprise Capture servers, CPT_Cluster, which includes these Managed Servers:

- WLS_CPT1 on WCCHOST1

- WLS_CPT2 on WCCHOST2

Applications for Capture

- capture

Data Sources for Capture

- `capture-ds`

- `capture-mds-ds`

- `mds-owsm`

- `opss-audit-viewDS`

- `opss-audit-DBDS`

- `opss-DBDS`

Startup and Shutdown Classes for Capture

- `oracle.jrf.AppContextStartup`

- `oracle.dms.wls.DMSStartup`

- `oracle.dms.wls.DMSShutdown`

- `oracle.as.jmx.framework.wls.spi.StartupListener`

- `oracle.ias.cache.Shutdown`

- `oracle.ias.cache.Startup`

- `oracle.security.jps.wls.JpsWlsStartupClass`

- `oracle.jrf.wls.JRFStartup`

- `oracle.core.ojdl.weblogic.ODLConfiguration`

- `oracle.j2ee.ws.server.WebServiceServerStartup`

B.6 Applications and Resources for the Administration Server

The following applications and resources are targeted to the Oracle WebLogic Server Administration Server, `AdminServer`, which runs on WCCHOST1 and WCCHOST2.

Applications for the Administration Server

- DMS Application (11.1.1.1.0)

- em

- FMW Welcome Page Application (11.1.0.0.0)

- EM (11.1.1)

- wsil-wls

Data Sources for the Administration Server

- mds-owsm

- mds-soa

- opss-audit-viewDS

- opss-audit-DBDS

- opss-DBDS

Startup and Shutdown Classes for the Administration Server

- oracle.jrf.AppContextStartup

- oracle.dms.wls.DMSStartup

- oracle.dms.wls.DMSShutdown

- oracle.as.jmx.framework.wls.spi.StartupListener

- oracle.ias.cache.Shutdown

- oracle.ias.cache.Startup

- oracle.security.jps.wls.JpsWlsStartupClass

- oracle.jrf.wls.JRFStartup

- oracle.core.ojdl.weblogic.ODLConfiguration

- oracle.j2ee.ws.server.WebServiceServerStartup

Index