# Oracle® Fusion Middleware

Enterprise Deployment Guide for Oracle WebCenter Portal

Release 12.2.1.1

**E73513-01**

November 2016

Documentation for administrators that describes how to install and configure Oracle Fusion Middleware components in an enterprise deployment.

ORACLE

Oracle Fusion Middleware Enterprise Deployment Guide for Oracle WebCenter Portal, Release 12.2.1.1

E73513-01



Primary Authors: Chuck Boucher (Writer), Frank Rizzo (MAA Engineer), Melwyn Paul (Writer), Abirami Sekar (QA)

# Contents

## 18 Using Whole Server Migration and Service Migration in an Enterprise Deployment



## 19 Configuring Single Sign-On for an Enterprise Deployment

# Preface

This guide explains how to install, configure, and manage a highly available Oracle Fusion Middleware enterprise deployment. For more information, see About the Enterprise Deployment Guide.



## Audience

In general, this document is intended for administrators of Oracle Fusion Middleware, who are assigned the task of installing and configuring Oracle Fusion Middleware software for production deployments.

Specific tasks can also be assigned to more specialized administrators, such as database administrators (DBAs) and network administrators, where applicable.

## 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. |

**Note:**

This guide focuses on the implementation of the enterprise deployment reference topology on Oracle Linux systems.

The topology can be implemented on any certified, supported operating system, but the examples in this guide typically show the commands and configuration steps as they should be performed using the bash shell on Oracle Linux.

# Part I

# Understanding an Enterprise Deployment

This part of the Enterprise Deployment Guide contains the following topics.

# 1

# Enterprise Deployment Overview

This chapter introduces the concept of an Oracle Fusion Middleware enterprise deployment.

It also provides information on when to use the Enterprise Deployment guide.



## 1.1 About the Enterprise Deployment Guide

An Enterprise Deployment Guide provides a comprehensive, scalable example for installing, configuring, and maintaining a secure, highly available, production-quality deployment of selected Oracle Fusion Middleware products. This resulting environment is known as an **enterprise deployment topology**.

By example, the enterprise deployment topology introduces key concepts and best practices that you can use to implement a similar Oracle Fusion Middleware environment for your organization.

Each Enterprise Deployment Guide provides detailed, validated instructions for implementing the reference topology. Along the way, the guide offers links to supporting documentation that explains concepts, reference material, and additional options for an Oracle Fusion Middleware enterprise deployment.

Note that the enterprise deployment topologies described in the enterprise deployment guides cannot meet the exact requirements of all Oracle customers. In some cases, you can consider alternatives to specific procedures in this guide, depending on whether the variations to the topology are documented and supported by Oracle.

Oracle recommends customers use the Enterprise Deployment Guides as a first option for deployment. If variations are required, then those variations should be verified by reviewing related Oracle documentation or by working with Oracle Support.

## 1.2 When to Use the Enterprise Deployment Guide

This guide describes one of three primary installation and configuration options for Oracle Fusion Middleware. Use this guide to help you plan, prepare, install, and

configure a multi-host, secure, highly available, production topology for selected Oracle Fusion Middleware products.

Alternatively, you can:

- Use the instructions in one of the product-specific installation guides to install and configure a **standard installation topology** for a selected set of Oracle Fusion Middleware products.

  A standard installation topology can be installed on a single host for evaluation purposes, but it can also serve as a starting point for scaling out to a more complex production environment.

  For Oracle WebCenter Portal, see:

  – *Installing and Configuring Oracle WebCenter Portal*

  For Oracle WebCenter Content , see:

  – *Installing and Configuring Oracle WebCenter Content*

  For Oracle SOA Suite, see:

  – *Installing SOA Suite and Business Process Management Quick Start for Developers*

- Review *Planning an Installation of Oracle Fusion Middleware*, which provides additional information to help you prepare for any Oracle Fusion Middleware installation.

# 2

# Understanding a Typical Enterprise Deployment

This chapter describes the general characteristics of a typical Oracle Fusion Middleware enterprise deployment. You can apply the concepts here to any product-specific enterprise deployment.

This chapter provides information on Enterprise Deployment Topology diagram.



## 2.1 Diagram of a Typical Enterprise Deployment

This section illustrates a typical enterprise deployment, including the Web tier, application tier, and data tier.

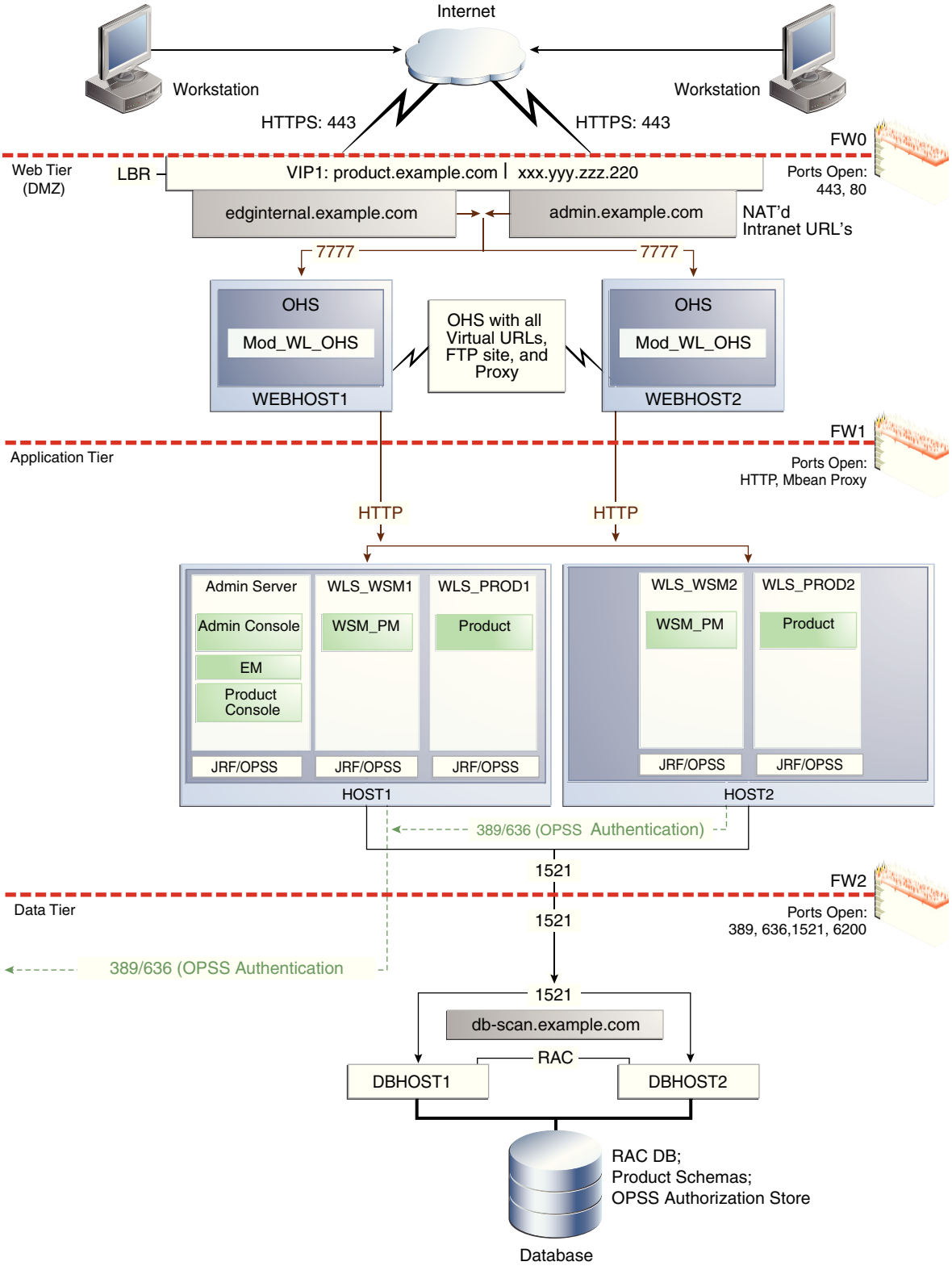
All Oracle Fusion Middleware enterprise deployments are designed to demonstrate the best practices for installing and configuring an Oracle Fusion Middleware production environment.

A best practices approach starts with the basic concept of a multi-tiered deployment and standard communications between the different software tiers.

Figure 2-1 shows a typical enterprise deployment, including the Web tier, application tier and data tier. All enterprise deployments are based on these basic principles.

For a description of each tier and the standard protocols used for communications within a typical Oracle Fusion Middleware enterprise deployment, see Understanding the Typical Enterprise Deployment Topology Diagram.

***Figure 2-1 Typical Enterprise Deployment Topology Diagram***




## 2.2 Understanding the Typical Enterprise Deployment Topology Diagram

This section provides a detailed description of the typical enterprise topology diagram.

### 2.2.1 Understanding the Firewalls and Zones of a Typical Enterprise Deployment

The topology is divided into several security zones, which are separated by firewalls:

- The Web tier (or DMZ), which is used for the hardware load balancer and Web servers (in this case, Oracle HTTP Server instances) that receive the initial requests from users. This zone is accessible only through a single virtual server name defined on the load balancer.
- The application tier, which is where the business and application logic resides.
- The data tier, which is not accessible from the Internet and reserved in this topology for the highly available database instances.

The firewalls are configured to allow data to be transferred only through specific communication ports. Those ports (or in some cases, the protocols that will need open ports in the firewall) are shown on each firewall line in the diagram.

For example:

- On the firewall protecting the Web tier, only the HTTP ports are open: 443 for HTTPS and 80 for HTTP.
- On the firewall protecting the Application tier, HTTP ports, and MBean proxy port are open.

  Applications that require external HTTP access can use the Oracle HTTP Server instances as a proxy. Note that this port for outbound communications only and the proxy capabilities on the Oracle HTTP Server must be enabled.
- On the firewall protecting the data tier, the database listener port (typically, 1521) must be open.

  The LDAP ports (typically, 389 and 636) are also required to be open for communication between the authorization provider and the LDAP-based identity store.

  The ONS port (typically, 6200) is also required so the application tier can receive notifications about workload and events in the Oracle RAC Database. These events are used by the Oracle WebLogic Server connection pools to adjust quickly (creating or destroying connections), depending on the availability and workload on the Oracle RAC database instances.

For a complete list of the ports you must open for a specific Oracle Fusion Middleware enterprise deployment topology, see the chapter that describes the topology you want to implement, or refer to the *Enterprise Deployment Workbook* for the topology you are implement. For more information, see Using the Enterprise Deployment Workbook .

## 2.2.2 Understanding the Elements of a Typical Enterprise Deployment Topology

The enterprise deployment topology consists of the following high-level elements:

- A hardware load balancer that routes requests from the Internet to the Web servers in the Web tier. It also routes requests from internal clients or other components that are performing internal invocations within the corporate network.
- A Web tier, consisting of a hardware load balancer and two or more physical computers that host the Web server instances (for high availability).

  The Web server instances are configured to authenticate users (via an external identity store and a single sign-on server) and then route the HTTP requests to the Oracle Fusion Middleware products and components running in the Application tier.

  The Web server instances also host static Web content that does not require application logic to be delivered. Placing such content in the Web tier reduces the overhead on the application servers and eliminates unnecessary network activity.
- An Application tier, consisting of two or more physical computers that are hosting a cluster of Oracle WebLogic Server Managed Servers, and the Administration Server for the domain. The Managed Servers are configured to run the various Oracle Fusion Middleware products, such as Oracle SOA Suite, Oracle Service Bus, Oracle WebCenter Content, and Oracle WebCenter Portal, depending on your choice of products in the enterprise deployment.
- A data tier, consisting of two or more physical hosts that are hosting an Oracle RAC Database.

## 2.2.3 Receiving Requests Through Hardware Load Balancer

The following topics describe the hardware load balancer and its role in an enterprise deployment.

Purpose of the Hardware Load Balancer (LBR)

Summary of the Typical Load Balancer Virtual Server Names

HTTPS versus HTTP Requests to the External Virtual Server Name

### 2.2.3.1 Purpose of the Hardware Load Balancer (LBR)

The following topics describe the types of requests handled by the hardware load balancer in an enterprise deployment.

HTTP Requests from the Internet to the Web server instances in the Web tier

Specific internal-only communications between the components of the Application tier

#### 2.2.3.1.1 HTTP Requests from the Internet to the Web server instances in the Web tier

The hardware load balancer balances the load on the Web tier by receiving requests to a single virtual host name and then routing each request to one of the Web server instances, based on a load balancing algorithm. In this way, the load balancer ensures that no one Web server is overloaded with HTTP requests.

For more information about the purpose of specific virtual host names on the hardware load balancer, see Summary of the Typical Load Balancer Virtual Server Names.

Note that in the reference topology, only HTTP requests are routed from the hardware load balancer to the Web tier. Secure Socket Layer (SSL) requests are terminated at the load balancer and only HTTP requests are forwarded to the Oracle HTTP Server instances. This guide does not provide instructions for SSL configuration between the load balancer and the Oracle HTTP Server instances or between the Web tier and the Application tier.

The load balancer provides high availability by ensuring that if one Web server goes down, requests will be routed to the remaining Web servers that are up and running.

Further, in a typical highly available configuration, the hardware load balancers are configured such that a hot standby device is ready to resume service in case a failure occurs in the main load balancing appliance. This is important because for many types of services and systems, the hardware load balancer becomes the unique point of access to make invocations and, as a result, becomes a single point of failure (SPOF) for the whole system if it is not protected.

#### 2.2.3.1.2 Specific internal-only communications between the components of the Application tier

In addition, the hardware load balancer routes specific communications between the Oracle Fusion Middleware components and applications on the application tier. The internal-only requests are also routed through the load balancer, using a unique virtual host name.

### 2.2.3.2 Summary of the Typical Load Balancer Virtual Server Names

In order to balance the load on servers and to provide high availability, the hardware load balancer is configured to recognize a set of virtual server names. As shown in the diagram, the following virtual server names are recognized by the hardware load balancer in this topology:

- `wcp.example.com` - This virtual server name is used for all incoming traffic.

  Users enter this URL to access the Oracle Fusion Middleware product you have deployed and the custom applications available on this server. The load balancer then routes these requests (using a load balancing algorithm) to one of the servers in the Web tier. In this way, the single virtual server name can be used to route traffic to multiple servers for load balancing and high availability of the Web servers instances.

- `wcpinternal.example.com` - This virtual server name is for internal communications only.

  The load balancer uses its **Network Address Translation (NAT)** capabilities to route any internal communication from the Application tier components that are directed to this URL. This URL is not exposed to external customers or users on the Internet. Each product has specific uses for the internal URL, so in the deployment instructions, we prefix it with the product name.

- `admin.example.com` - This virtual server name is for administrators who need to access the Oracle Enterprise Manager Fusion Middleware Control and Oracle WebLogic Server Administration Console interfaces.

  This URL is known only to internal administrators. It also uses the NAT capabilities of the load balancer to route administrators to the active Administration Server in the domain.

For the complete set of virtual server names you must define for your topology, see the the chapter that describes the product-specific topology.

#### 2.2.3.3 HTTPS versus HTTP Requests to the External Virtual Server Name

Note that when you configure the hardware load balancer, a best practice is to assign the main external URL (for example, `http://myapplication.example.com`) to port 80 and port 443.

Any request on port 80 (non-SSL protocol) should be redirected to port 443 (SSL protocol). Exceptions to this rule include requests from public WSDLs. For more information, see Configuring Virtual Hosts on the Hardware Load Balancer.

### 2.2.4 Understanding the Web Tier

The Web tier of the reference topology consists of the Web servers that receive requests from the load balancer. In the typical enterprise deployment, at least two Oracle HTTP Server instances are configured in the Web tier. The following topics provide more detail.

Benefits of Using Oracle HTTP Server Instances to Route Requests

Alternatives to Using Oracle HTTP Server in the Web Tier

Configuration of Oracle HTTP Server in the Web Tier

About Mod_WL_OHS

#### 2.2.4.1 Benefits of Using Oracle HTTP Server Instances to Route Requests

A Web tier with Oracle HTTP Server is not a requirement for many of the Oracle Fusion Middleware products. You can route traffic directly from the hardware load balancer to the WLS servers in the Application Tier. However, a Web tier does provide several advantages, which is why it is recommended as part of the reference topology:

- The Web tier provides DMZ public zone, which is a common requirement in security audits. If a load balancer routes directly to the WebLogic Server, requests move from the load balancer to the application tier in one single HTTP jump, which can cause security concerns.
- The Web tier allows the WebLogic Server cluster membership to be reconfigured (new servers added, others removed) without having to change the Web server configuration (as long as at least some of the servers in the configured list remain alive).
- Oracle HTTP Server delivers static content more efficiently and faster than WebLogic Server; it also provides FTP services, which are required for some enterprise deployments, as well as the ability to create virtual hosts and proxies via the Oracle HTTP Server configuration files.
- Oracle HTTP Server provides HTTP redirection over and above what WebLogic Server provides. You can use Oracle HTTP Server as a front end against many different WebLogic Server clusters, and in some cases, control the routing via content based routing.
- Oracle HTTP Server provides the ability to integrate single sign-on capabilities into your enterprise deployment. For example, you can later implement single sign-on for the enterprise deployment, using Oracle Access Manager, which is part of the Oracle Identity and Access Management family of products.

- Oracle HTTP Server provides support for WebSocket connections deployed within WebLogic Server.

For more information about Oracle HTTP Server, see Introduction to Oracle HTTP Server in *Administrator's Guide for Oracle HTTP Server*.

#### 2.2.4.2 Alternatives to Using Oracle HTTP Server in the Web Tier

Although Oracle HTTP Server provides a variety of benefits in an enterprise topology, Oracle also supports routing requests directly from the hardware load balancer to the Managed Servers in the middle tier.

This approach provide the following advantages:

- Lower configuration and processing overhead than using a front-end Oracle HTTP Server Web tier front-end.
- Monitoring at the application level since the LBR can be configured to monitor specific URLS for each Managed Server (something that is not possible with OHS).

  Note that this enables routing to the Managed Servers only when all composites are deployed, and you must use the appropriate monitoring software.

#### 2.2.4.3 Configuration of Oracle HTTP Server in the Web Tier

Starting with Oracle Fusion Middleware 12*c*, the Oracle HTTP Server software can be configured in one of two ways: as part of an existing Oracle WebLogic Server domain or in its own standalone domain. Each configuration offers specific benefits.

When you configure Oracle HTTP Server instances as part of an existing WebLogic Server domain, you can manage the Oracle HTTP Server instances, including the wiring of communications between the Web servers and the Oracle WebLogic Server Managed Servers using Oracle Enterprise Manager Fusion Middleware Control. When you configure Oracle HTTP Server in a standalone configuration, you can configure and manage the Oracle HTTP Server instances independently of the application tier domains.

For this enterprise deployment guide, the Oracle HTTP Server instances are configured as separate standalone domains, one on each Web tier host. You can choose to configure the Oracle HTTP Server instances as part of the application tier domain, but this enterprise deployment guide does not provide specific steps to configure the Oracle HTTP Server instances in that manner.

For more information, see "Understanding Oracle HTTP Server Installation Options" in *Installing and Configuring Oracle HTTP Server*.

#### 2.2.4.4 About Mod_WL_OHS

As shown in the diagram, the Oracle HTTP Server instances use the WebLogic Proxy Plug-In (`mod_wl_ohs`) for proxying HTTP requests from Oracle HTTP Server to the Oracle WebLogic Server Managed Servers in the Application tier.

For more information, see Overview of Web Server Proxy Plug-In in *Using Oracle WebLogic Server Proxy Plug-Ins 12.2.1.1.0*.

### 2.2.5 Understanding the Application Tier

The application tier consists of two physical host computers, where Oracle WebLogic Server and the Oracle Fusion Middleware products are installed and configured. The application tier computers reside in the secured zone between firewall 1 and firewall 2.

The following topics provide more information.

Configuration of the Administration Server and Managed Servers Domain Directories

Using Oracle Web Services Manager in the Application Tier

Best Practices and Variations on the Configuration of the Clusters and Hosts on the Application Tier

About the Node Manager Configuration in a Typical Enterprise Deployment

About Using Unicast for Communications Within the Application Tier

Understanding OPSS and Requests to the Authentication and Authorization Stores

#### 2.2.5.1 Configuration of the Administration Server and Managed Servers Domain Directories

Unlike the Managed Servers in the domain, the Administration Server uses an active-passive high availability configuration. This is because only one Administration Server can be running within an Oracle WebLogic Server domain.

In the topology diagrams, the Administration Server on HOST1 is in the active state and the Administration Server on HOST2 is in the passive (inactive) state.

To support the manual fail over of the Administration Server in the event of a system failure, the typical enterprise deployment topology includes:

- A Virtual IP Address (VIP) for the routing of Administration Server requests
- The configuration of the Administration Server domain directory on a shared storage device.

In the event of a system failure (for example a failure of HOST1), you can manually reassign the Administration Server VIP address to another host in the domain, mount the Administration Server domain directory on the new host, and then start the Administration Server on the new host.

However, unlike the Administration Server, there is no benefit to storing the Managed Servers on shared storage. In fact, there is a potential performance impact when Managed Server configuration data is not stored on the local disk of the host computer.

As a result, in the typical enterprise deployment, after you configure the Administration Server domain on shared storage, a copy of the domain configuration is placed on the local storage device of each host computer, and the Managed Servers are started from this copy of the domain configuration. You create this copy using the Oracle WebLogic Server pack and unpack utilities.

The resulting configuration consists of separate domain directories on each host: one for the Administration Server (on shared storage) and one for the Managed Servers (on local storage). Depending upon the action required, you must perform configuration tasks from one domain directory or the other.

For more information about structure of the Administration Server domain directory and the Managed Server domain directory, as well as the variables used to reference these directories, see Understanding the Recommended Directory Structure for an Enterprise Deployment.

There is an additional benefit to the multiple domain directory model. It allows you to isolate the Administration Server from the Managed Servers. By default, the primary enterprise deployment topology assumes the Administration Server domain directory is on one of the Application Tier hosts, but if necessary, you could isolate the Administration Server further by running it from its own host, for example in cases where the Administration Server is consuming high CPU or RAM. Some administrators prefer to configure the Administration Server on a separate, dedicated host, and the multiple domain directory model makes that possible.

#### 2.2.5.2 Using Oracle Web Services Manager in the Application Tier

Oracle Web Services Manager (Oracle WSM) provides a policy framework to manage and secure Web services in the Enterprise Deployment topology.

In most enterprise deployment topologies, the Oracle Web Services Manager Policy Manager runs on Managed Servers in a separate cluster, where it can be deployed in an active-active highly available configuration.

You can choose to target Oracle Web Services Manager and Fusion Middleware products or applications to the same cluster, as long as you are aware of the implications.

The main reasons for deploying Oracle Web Services Manager on its own managed servers is to improve performance and availability isolation. Oracle Web Services Manager often provides policies to custom Web services or to other products and components in the domain. In such a case, you do not want the additional Oracle Web Services Manager activity to affect the performance of any applications that are sharing the same managed server or cluster as Oracle Web Services Manager.

The eventual process of scaling out or scaling up is also better addressed when the components are isolated. You can scale out or scale up only the Fusion Middleware application Managed Servers where your products are deployed or only the Managed Servers where Oracle Web Services Manager is deployed, without affecting the other product.

#### 2.2.5.3 Best Practices and Variations on the Configuration of the Clusters and Hosts on the Application Tier

In a typical enterprise deployment, you configure the Managed Servers in a cluster on two or more hosts in the application tier. For specific Oracle Fusion Middleware products, the enterprise deployment reference topologies demonstrate best practices for the number of Managed Servers, the number of clusters, and what services are targeted to each cluster.

These best practices take into account typical performance, maintenance, and scale-out requirements for each product. The result is the grouping of Managed Servers into an appropriate set of clusters within the domain.

Variations of the enterprise deployment topology allow the targeting of specific products or components to additional clusters or hosts for improved performance and isolation.

For example, you can consider hosting the Administration Server on a separate and smaller host computer, which allows the FMW components and products to be isolated from the Administration Server.

These variations in the topology are supported, but the enterprise deployment reference topology uses the minimum hardware resources while keeping high availability, scalability and security in mind. You should perform the appropriate resource planning and sizing, based on the system requirements for each type of

server and the load that the system needs to sustain. Based on these decisions, you must adapt the steps to install and configure these variations accordingly from the instructions presented in this guide.

#### 2.2.5.4 About the Node Manager Configuration in a Typical Enterprise Deployment

Starting with Oracle Fusion Middleware 12*c*, you can use either a per domain Node Manager or a per host Node Manager. The following sections of this topic provide more information on the impact of the Node Manager configuration on a typical enterprise deployment.

---

**Note:**

For general information about these two types of Node Managers, see Overview in *Administering Node Manager for Oracle WebLogic Server*.

---

##### About Using a Per Domain Node Manager Configuration

In a per domain Node Manager configuration—as opposed to a per host Node Manager configuration—you actually start two Node Manager instances on the Administration Server host: one from the Administration Server domain directory and one from the Managed Servers domain directory. In addition, a separate Node Manager instance runs on each of the other hosts in the topology.

The Node Manager controlling the Administration Server uses the listen address of the virtual host name created for the Administration Server. The Node Manager controlling the Managed Servers uses the listen address of the physical host. When the Administration Server fails over to another host, an additional instance of Node Manager is started to control the Administration Server on the failover host.

The key advantages of the per domain configuration are an easier and simpler initial setup of the Node Manager and the ability to set Node Manager properties that are unique to the Administration Server. This last feature was important in previous releases because some features, such as Crash Recovery, applied only to the Administration Server and not to the Managed servers. In the current release, the Oracle SOA Suite products can be configured for Automated Service Migration, rather than Whole Server Migration. This means the Managed Servers, as well as the Administration Server, can take advantage of Crash Recovery, so there is no need to apply different properties to the Administration Server and Managed Server domain directories.

Another advantage is that the per domain Node Manager provides a default SSL configuration for Node Manager-to-Server communication, based on the Demo Identity store created for each domain.

##### About Using a Per Host Domain Manager Configuration

In a per-host Node Manager configuration, you start a single Node Manager instance to control the Administration Server and all Managed Servers on a host, even those that reside in different domains. This reduces the footprint and resource utilization on the Administration Server host, especially in those cases where multiple domains coexist on the same machine.

A per-host Node Manager configuration allows all Node Managers to use a listen address of ANY, so they listen on all addresses available on the host. This means that when the Administration Server fails over to a new host, no additional configuration is

necessary. The per host configuration allows for simpler maintenance, because you can update and maintain a single Node Manager properties file on each host, rather than multiple node manager property files.

The per-host Node Manager configuration requires additional configuration steps. If you want SSL for Node Manager-to-Server communication, then you must configure an additional Identity and Trust store, and it also requires using Subject Alternate Names (SAN), because the Node Manager listens on multiple addresses. Note that SSL communications are typically not required for the application tier, because it is protected by two firewalls.

#### 2.2.5.5 About Using Unicast for Communications Within the Application Tier

Oracle recommends the unicast communication protocol for communication between the Managed Servers and hosts within the Oracle WebLogic Server clusters in an enterprise deployment. 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.

When you consider using the multicast or unicast protocol for your own deployment, consider the type of network, the number of members in the cluster, and the reliability requirements for cluster membership. Also consider the following benefits of each protocol.

**Benefits of unicast in an enterprise deployment:**

- Uses a group leader that every server sends messages directly to. This leader is responsible for retransmitting the message to every other group member and other group leaders, if applicable.
- Works out of the box in most network topologies
- Requires no additional configuration, regardless of the network topology.
- Uses a single missed heartbeat to remove a server from the cluster membership list.

**Benefits of multicast in an enterprise deployment:**

- Multicast uses a more scalable peer-to-peer model where a server sends each message directly to the network once and the network makes sure that each cluster member receives the message directly from the network.
- Works out of the box in most modern environments where the cluster members are in a single subnet.
- Requires additional configuration in the router(s) and WebLogic Server (that is., Multicast TTL) if the cluster members span more than one subnet.
- Uses three consecutive missed heartbeats to remove a server from the cluster membership list.

Depending on the number of servers in your cluster and on whether the cluster membership is critical for the underlying application (for example in session-replication intensive applications or clusters with intensive RMI invocations across the cluster), each model may behave better.

Consider whether your topology is going to be part of an Active-Active disaster recovery system or if the cluster is going to traverse multiple subnets. In general, unicast will behave better in those cases.

For more information see the following resources:

- "Configuring Multicast Messaging for WebLogic Server Clusters" in the *High Availability Guide*
- "One-to-Many Communication Using Unicast" in *Administering Clusters for Oracle WebLogic Server*.

#### 2.2.5.6 Understanding OPSS and Requests to the Authentication and Authorization Stores

Many of the Oracle Fusion Middleware products and components require an Oracle Platform Security Services (OPSS) security store for authentication providers (an identity store), policies, credentials, keystores, and for audit data. As a result, communications must be enabled so the Application tier can send requests to and from the security providers.

For authentication, this communication is to an LDAP directory, such as Oracle Internet Directory (OID) or Oracle Unified Directory (OUD), which typically communicates over port 389 or 636. When you configure an Oracle Fusion Middleware domain, the domain is configured by default to use the WebLogic Server Authentication provider. However, for an enterprise deployment, you must use a dedicated, centralized LDAP-compliant authentication provider.

For authorization (and the policy store), the location of the security store varies, depending upon the tier:

- For the application tier, the authorization store is database-based, so frequent connections from the Oracle WebLogic Server Managed Servers to the database are required for the purpose of retrieving the required OPSS data.
- For the Web tier, the authorization store is file-based, so connections to the database are not required.

For more information about OPSS security stores, see the following sections of *Securing Applications with Oracle Platform Security Services*:

- "Authentication Basics"
- "The OPSS Policy Model"

### 2.2.6 About the Data Tier

In the Data tier, an Oracle RAC database runs on the two hosts (DBHOST1 and DBHOST2). The database contains the schemas required by the Oracle WebCenter Portal components and the Oracle Platform Security Services (OPSS) policy store.

You can define multiple services for the different products and components in an enterprise deployment to isolate and prioritize throughput and performance accordingly. In this guide, one database service is used as an example. Furthermore, you can use other high availability database solutions to protect the database:

- Oracle Data Guard; for more information, see the *Oracle Data Guard Concepts and Administration*
- Oracle RAC One Node; for more information, see "Overview of Oracle RAC One Node" in the *Oracle Real Application Clusters Administration and Deployment Guide*

These solutions above provide protection for the database beyond the information provided in this guide, which focuses on using an Oracle RAC Database, given the

scalability and availability requirements that typically apply to an enterprise deployment.

For more information about using Oracle Databases in a high availability environment, see "Database Considerations" in the *High Availability Guide*.

# 3

# Understanding the WebCenter Portal Enterprise Deployment Topology

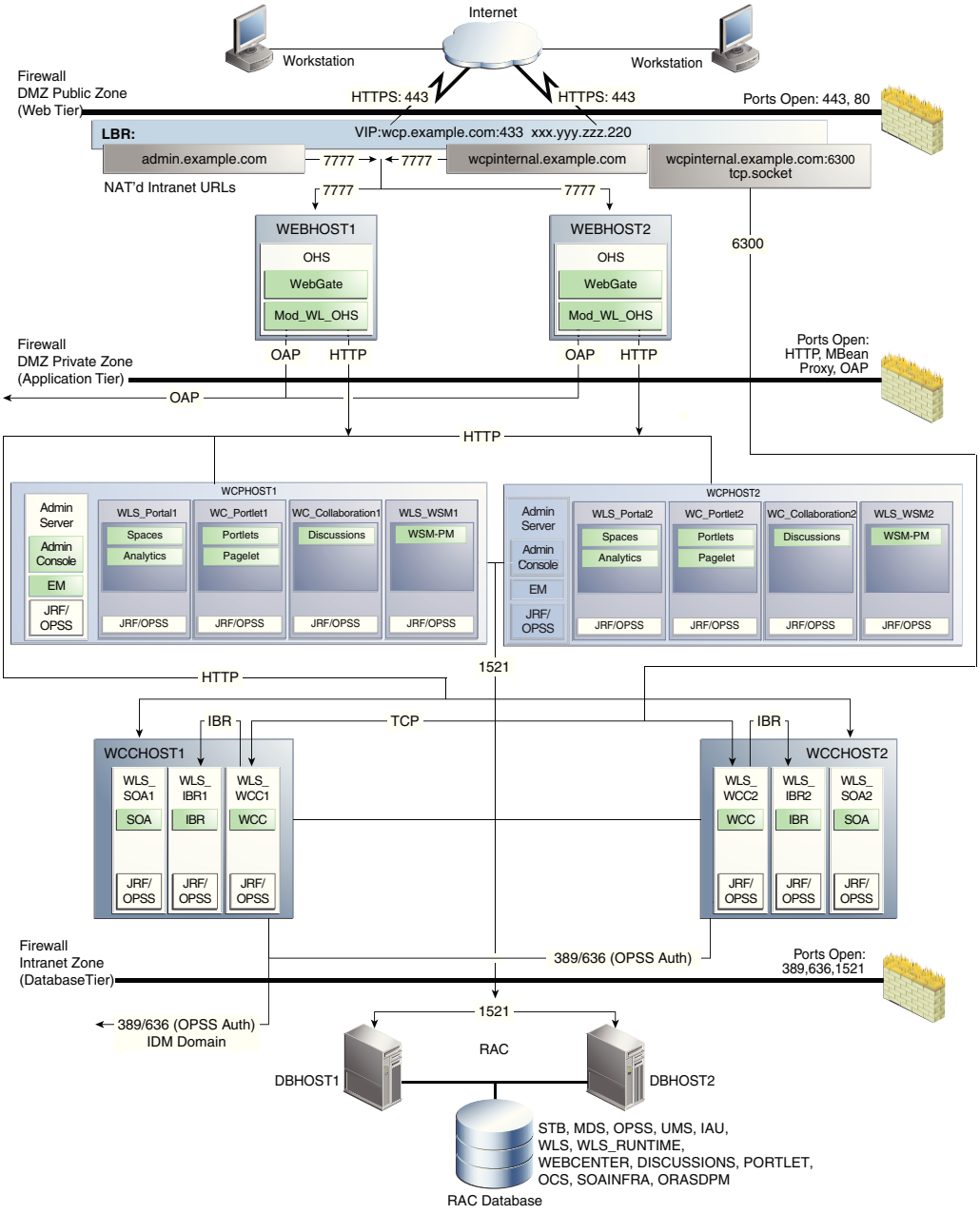
This chapter describes the WebCenter Portal deployment topologies. These topologies represent specific reference implementations of the concepts described in Understanding a Typical Enterprise Deployment.

This chapter provides information on primary WebCenter Portal topology diagrams.



## 3.1 Diagram of the WebCenter Portal Enterprise Deployment Topology

The following diagram shows the primary Oracle WebCenter Portal enterprise deployment topology, which is described in this guide.




# 3.2 Understanding the Primary WebCenter Portal Topology Diagrams

The Oracle WebCenter Portal topology follows a standard approach to an enterprise topology based on Oracle-recommended best practices. The standard elements of an Oracle Fusion Middleware enterprise topology are described in detail in Understanding a Typical Enterprise Deployment.

Before you review the information here, it is assumed you have reviewed the information in Understanding a Typical Enterprise Deployment and that you are familiar with the general concepts of an enterprise deployment topology.

See the following sections for information about the elements that are unique to the topology described in this chapter:

Summary of the WebCenter Portal Load Balancer Virtual Server Names

Summary of the Managed Servers and Clusters on the WebCenter Portal Application Tier

### 3.2.1 Summary of the WebCenter Portal Load Balancer Virtual Server Names

In order to balance the load on servers and to provide high availability, the hardware load balancer is configured to recognize a set of virtual server names.

For information about the purpose of each of these server names, see Summary of the Typical Load Balancer Virtual Server Names.

The following virtual server names are recognized by the hardware load balancer in Oracle WebCenter Portal topologies:

- `wcp.example.com` — This virtual server name is used for all incoming traffic. It acts as the access point for all HTTP traffic to the run-time WebCenter Portal components. The load balancer listens for all requests to this virtual server name over SSL. As a result, clients access this service using the following secure address:

  ```
  wcp.example.com:443
  ```

- wcpinternal.example.com — This virtual server name is used for internal calls to Oracle WebCenter services. There are two VIPs configured at the hardware load balancer. One (listening on port 80) is used for web-based services. The second (listening on port 6300) is for WebCenter Conent Remote Intradoc Client (RIDC) API calls.

  Incoming traffic from clients is not SSL-enabled. Clients accessing the HTTP services use the following address. These requests are forwarded to port 7777 on WEBHOST1 and WEBHOST2:

  ```
  http://wcpinternal.example.com:80/...
  ```

  WebCenter Content RIDC-enabled applications, such as the WebCenter Content Desktop Integration Suite (DIS) and WebCenter Portal Document Services, use port 6300 for TCP connections to WebCenter Content Server's RIDC API endpoints. These requests are forwarded to port 4444 on WCPHOST1 and WCCHOST2:

  ```
  wcpinternal.example.com:6300
  ```

- `admin.example.com` - This virtual server name is for administrators who need to access the Oracle Enterprise Manager Fusion Middleware Control and Oracle WebLogic Server Administration Console interfaces.

  ```
  http://admin.example.com:80/...
  ```

Use instructions later in this guide to perform the following tasks:

- Configure the hardware load balancer to recognize and route requests to the virtual host names
- Configure the Oracle HTTP Server instances on the Web Tier to recognize and properly route requests to these virtual host names to the correct host computers.

### 3.2.2 Summary of the Managed Servers and Clusters on the WebCenter Portal Application Tier

The Application tier hosts the Administration Server and Managed Servers in the Oracle WebLogic Server domain.

Depending upon the topology you select, the Oracle WebLogic Server domain for the domain consists of the clusters shown in Summary of the Managed Servers and Clusters on the WebCenter Portal Application Tier. These clusters function as active-active high availability configurations.

***Table 3-1 Summary of the Clusters in the Oracle WebCenter Portal Enterprise Deployment Topology***

| Product Component | Cluster | Managed Servers |
|---|---|---|
| Oracle Web Services Manager | WSM-PM_Cluster | WLS_WSM1, WLS_WSM2 |
| Oracle WebCenter Portal | Portal_Cluster | WLS_Portal1, WLS_Portal2 |
| Oracle WebCenter Portlet | Portlet_Cluster | WLS_Portlet1, WLS_Portlet2 |
| Oracle WebCenter Collaboration | Collab_Cluster | WLS_Collaboration1, WLS_Collaboration2 |
| Oracle WebCenter Content | WCC_Cluster | WLS_CC1, WLS_CC2 |
| Oracle Inbound Refinery | IBR_Servers | WLS_IBR1, WLS_IBR2 |
| Oracle SOA Suite | SOA_Cluster | WLS_SOA1, WLS_SOA2 |

## 3.3 Flow Charts and Roadmaps for Implementing the Primary WebCenter Portal Enterprise Topologies

The following topics summarize the high-level steps you must perform to install and configure the enterprise topology described in this chapter.

Flow Chart of the Steps to Install and Configure the WebCenter Portal Enterprise Topologies

Roadmap Table for Planning and Preparing for an Enterprise Deployment

Roadmap Table for Configuring the Oracle WebCenter Portal Topology

### 3.3.1 Flow Chart of the Steps to Install and Configure the WebCenter Portal Enterprise Topologies

The following flow chart shows the steps required to install and configure the primary enterprise deployment topologies described in this chapter. The sections following the flow chart explain each step in the flow chart.

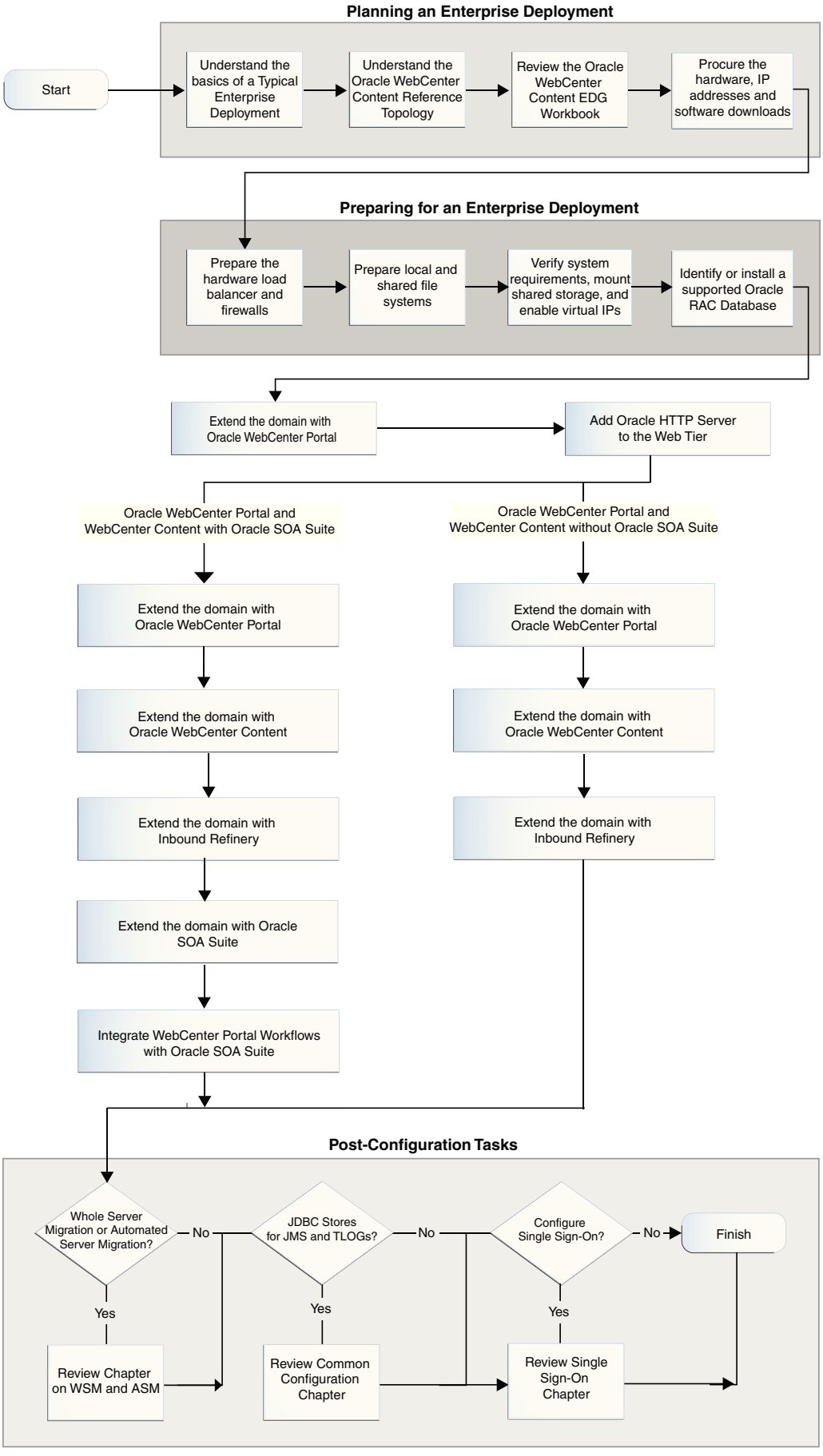
This guide is designed so you can start with a working WebCenter Portal domain and then later extend the domain to add additional capabilities.

This modular approach to building the topology allows you to make strategic decisions, based on your hardware and software resources, as well as the Oracle WebCenter Portal features that are most important to your organization.

It also allows you to validate and troubleshoot each individual product or component as they are configured.

This does not imply that configuring multiple products in one Configuration Wizard session is not supported; it is possible to group various extensions like the ones presented in this guide in one Configuration Wizard execution. However, the

instructions in this guide focus primarily on the modular approach to building an enterprise deployment.


Planning an Enterprise Deployment
Start
Understand the basics of a Typical Enterprise Deployment
Understand the Oracle WebCenter Content Reference Topology
Review the Oracle WebCenter Content EDG Workbook
Procure the hardware, IP addresses and software downloads
Preparing for an Enterprise Deployment
Prepare the hardware load balancer and firewalls
Prepare local and shared file systems
Verify system requirements, mount shared storage, and enable virtual IPs
Identify or install a supported Oracle RAC Database
Extend the domain with Oracle WebCenter Portal
Add Oracle HTTP Server to the Web Tier
Oracle WebCenter Portal and WebCenter Content with Oracle SOA Suite
Oracle WebCenter Portal and WebCenter Content without Oracle SOA Suite
Extend the domain with Oracle WebCenter Portal
Extend the domain with Oracle WebCenter Content
Extend the domain with Inbound Refinery
Extend the domain with Oracle SOA Suite
Integrate WebCenter Portal Workflows with Oracle SOA Suite
Extend the domain with Oracle WebCenter Portal
Extend the domain with Oracle WebCenter Content
Extend the domain with Inbound Refinery
Post-Configuration Tasks
Whole Server Migration or Automated Server Migration?
No
Yes
Review Chapter on WSM and ASM
JDBC Stores for JMS and TLOGs?
No
Yes
Review Common Configuration Chapter
Configure Single Sign-On?
No
Yes
Review Single Sign-On Chapter
Finish

### 3.3.2 Roadmap Table for Planning and Preparing for an Enterprise Deployment

The following table describes each of the planning and preparing steps shown in the enterprise topology flow chart.

| Flow Chart Step | More Information |
|---|---|
| Understand the basics of a Typical Enterprise Deployment | Understanding a Typical Enterprise Deployment |
| Understand the specific reference topology for the products you plan to deploy. | Review the product-specific topologies and the description of the topologies, including the virtual servers required and the summary of clusters and Managed Servers recommended for the product-specific deployment. |
| Review the Oracle WebCenter Portal EDG Workbook | Using the Enterprise Deployment Workbook |
| Procure the hardware, IP addresses and software downloads | Procuring Resources for an Enterprise Deployment |
| Prepare the hardware load balancer and firewalls | Preparing the Load Balancer and Firewalls for an Enterprise Deployment |
| Prepare the file system | Preparing the File System for an Enterprise Deployment |
| Verify system requirements, mount shared storage, and enable virtual IPs | Preparing the Host Computers for an Enterprise Deployment |
| Identify or install a supported Oracle RAC Database | Preparing the Database for an Enterprise Deployment |

### 3.3.3 Roadmap Table for Configuring the Oracle WebCenter Portal Topology

Roadmap Table for Configuring the WebCenter Portal Enterprise Topology describes each of the configuration steps required when configuring the topology shown in Diagram of the WebCenter Portal Enterprise Deployment Topology.

These steps correspond to the steps shown in the flow chart in Flow Chart of the Steps to Install and Configure the WebCenter Portal Enterprise Topologies.

***Table 3-2 Roadmap Table for Configuring the Oracle WebCenter Portal Topology***

| Flow Chart Step | More Information |
|---|---|
| Create the initial Infrastructure domain | Creating the Initial Infrastructure Domain for an Enterprise Deployment |
| Extend the domain to Include the Web Tier | Configuring the Web Tier for an Enterprise Deployment |
| Extend the domain with Oracle WebCenter Portal | Extending the Domain with Oracle WebCenter Portal |
| Extend the domain with Oracle WebCenter Content | Extending the Domain to Include Oracle WebCenter Content |
| Extend the domain with Inbound Refinery | Extending the Domain to Include Inbound Refinery |
| Extend the domain with Oracle SOA Suite | Extending the Domain with Oracle SOA Suite |
| Integrating WebCenter Portal with Oracle SOA Suite in the Same Domain | Integrating WebCenter Portal Workflows with Oracle SOA Suite in the Same Domain |

# Part II

# Preparing for an Enterprise Deployment

This part of the enterprise deployment guide contains the following topics.

# 4

# Using the Enterprise Deployment Workbook

This chapter introduces the Enterprise Deployment Workbook; it describes how you can use the workbook to plan an enterprise deployment for your organization.

This chapter provides an introduction to the Enterprise Deployment workbook, use cases and information on who should use the Enterprise Deployment workbook.



## 4.1 Introduction to the Enterprise Deployment Workbook

This section provides a brief introduction of the enterprise deployment workbook.

The Oracle Fusion Middleware Enterprise Deployment Workbook is a companion document to this guide. It is a spreadsheet that can be used by architects, system engineers, database administrators, and others to plan and record all the details for an environment installation (such as server names, URLs, port numbers, installation paths, and other resources).

The Enterprise Deployment Workbook serves as a single document you can use to track input variables for the entire process, allowing for:

- Separation of tasks between architects, system engineers, database administrators, and other key organizational roles
- Comprehensive planning before the implementation
- Validation of planned decisions before actual implementation
- Consistency during implementation

- A record of the environment for future use

## 4.2 Typical Use Case for Using the Workbook

This section lists the roles and tasks involved in a typical use case of the enterprise deployment workbook.

A typical use case for the Enterprise Deployment Workbook involves the following roles and tasks, in preparation for an Oracle Fusion Middleware enterprise deployment:

- Architects read through the first five chapters of this guide, and fill in the corresponding sections of the Workbook.
- The Workbook is validated by other architects and system engineers.
- The architect uses the validated workbook to initiate network and system change requests with system engineering departments;
- The Administrators and System Integrators who are installing and configuring the software refer to the workbook and the subsequent chapters of this guide to perform the installation and configuration tasks.

## 4.3 Using the Oracle WebCenter Portal Enterprise Deployment Workbook

This section provides details for using the enterprise deployment workbook.

The following sections provide an introduction to the location and contents of the Oracle WebCenter Portal Enterprise Deployment Workbook:

Locating the Oracle WebCenter Portal Enterprise Deployment Workbook

Understanding the Contents of the Oracle WebCenter Portal Enterprise Deployment Workbook

### 4.3.1 Locating the Oracle WebCenter Portal Enterprise Deployment Workbook

The Oracle WebCenter Portal Enterprise Deployment Workbook is available as a Microsoft Excel Spreadsheet in the Oracle Fusion Middleware documentation library. It is available as a link on the Install, Patch, and Upgrade page of the library.

### 4.3.2 Understanding the Contents of the Oracle WebCenter Portal Enterprise Deployment Workbook

The following sections describe the contents of the Oracle WebCenter Portal Enterprise Deployment Workbook. The workbook is divided into tabs, each containing a set of related variables and values you will need to install and configure the Enterprise Deployment topologies.

Using the Start Tab

Using the Hardware - Host Computers Tab

Using the Network - Virtual Hosts & Ports Tab

Using the Storage - Directory Variables Tab

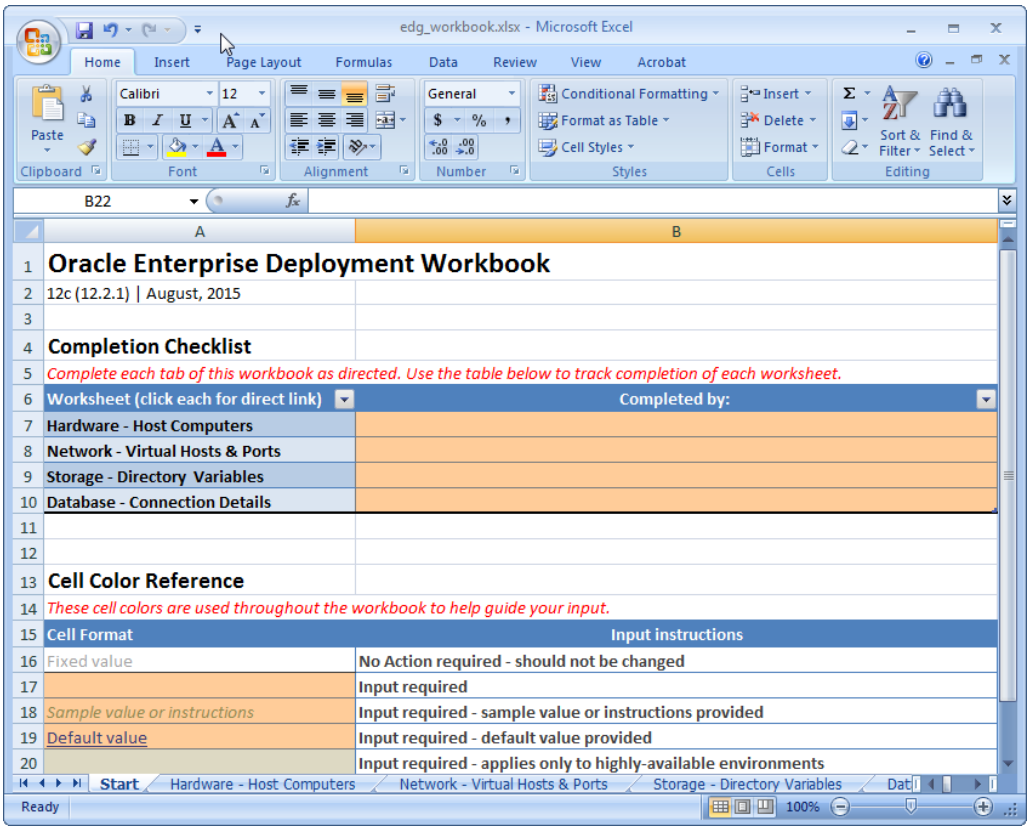
Using the Database - Connection Details Tab

#### 4.3.2.1 Using the Start Tab

The Start tab of the Enterprise Deployment Workbook serves as a table of contents for the rest of the workbook. You can also use it to identify the people who will be completing the spreadsheet.

The Start tab also provides a key to identify the colors used to identify workbook fields that need values, as well as those that are provided for informational purposes.

The following image shows the Start tab of the spreadsheet.




#### 4.3.2.2 Using the Hardware - Host Computers Tab

The Hardware - Host Computers tab lists the host computers required to install and configure the Oracle WebCenter Portal Enterprise Deployment Topology.

The reference topologies typically require a minimum of six host computers: two for the Web tier, two for the application tier, and two for the Oracle RAC database on the data tier. If you decide to expand the environment to include more systems, add a row for each additional host computer.

The **Abstract Host Name** is the name used throughout this guide to reference the host. For each row, procure a host computer, and enter the **Actual Host Name**. You can then use the actual host name when any of the abstract names is referenced in this guide.

For example, if a procedure in this guide references WCPHOST1, you can then replace the WCPHOST1variable with the actual name provided on the Hardware - Host Computers tab of the workbook.

For easy reference, Oracle also recommends that you include the IP address, Operating System (including the version), number of CPUs, and the amount of RAM for each host. This information can be useful during the installation, configuration, and maintenance of the enterprise deployment.

For more information, see Preparing the Host Computers for an Enterprise Deployment.

#### 4.3.2.3 Using the Network - Virtual Hosts & Ports Tab

The Network - Virtual Hosts & Ports tab lists the virtual hosts that must be defined by your network administrator before you can install and configure the enterprise deployment topology.

The port numbers are important for several reasons. You must have quick reference to the port numbers so you can access the management consoles; the firewalls must also be configured to allow network traffic via specific ports.

Each virtual host, virtual IP address, and each network port serves a distinct purpose in the deployment. For more information, see Preparing the Load Balancer and Firewalls for an Enterprise Deployment.

In the Network - Virtual Hosts table, review the items in the **Abstract Virtual Host or Virtual IP Name** column. These are the virtual host and virtual IP names used in the procedures in this guide. For each abstract name, enter the actual virtual host name defined by your network administrator. Whenever this guide references one of the abstract virtual host or virtual IP names, replace that value with the actual corresponding value in this table.

Similarly, in many cases, this guide assumes you are using default port numbers for the components or products you install and configure. However, in reality, you will likely have to use different port numbers. Use the Network - Port Numbers table to map the default port values to the actual values used in your specific installation.

#### 4.3.2.4 Using the Storage - Directory Variables Tab

As part of preparing for an enterprise deployment, it is assumed you will be using a standard directory structure, which is recommended for Oracle enterprise deployments.

In addition, procedures in this book reference specific directory locations. Within the procedures, each directory is assigned a consistent variable, which you should replace with the actual location of the directory in your installation.

For each of the directory locations listed on this tab, provide the actual directory path in your installation.

In addition, for the application tier, it is recommended that many of these standard directories be created on a shared storage device. For those directories, the table also provides fields so you can enter the name of the shared storage location and the mount point used when you mounted the shared location.

For more information, see Preparing the File System for an Enterprise Deployment.

#### 4.3.2.5 Using the Database - Connection Details Tab

When you are installing and configuring the enterprise deployment topology, you will often have to make connections to a highly available Oracle Real Application Clusters (RAC) database. In this guide, the procedures reference a set of variables that identify the information you will need to provide to connect to the database from tools, such as the Configuration Wizard and the Repository Creation Utility.

To be sure you have these values handy, use this tab to enter the actual values for these variables in your database installation.

For more information, see Preparing the Database for an Enterprise Deployment.

## 4.4 Who Should Use the Enterprise Deployment Workbook?

The information in the Enterprise Deployment Workbook is divided into categories. Depending on the structure of your organization and roles defined for your team, you can assign specific individuals in your organization to fill in the details of the workbook. Similarly the information in each category can be assigned to the individual or team responsible for planning, procuring, or setting up each category of resources.

For example, the workbook can be filled in, reviewed, and used by people in your organization that fill the following roles:

- Information Technology (IT) Director
- Architect
- System Administrator
- Network Engineer
- Database Administrator

# 5

# Procuring Resources for an Enterprise Deployment

Use the following topics to procure the required hardware, software, and network settings before you begin configuring the Oracle WebCenter Portal reference topology.

This chapter provides information on reserving the required IP addresses and identifying and obtaining software downloads for an enterprise deployment.

Hardware and Software Requirements for the Enterprise Deployment Topology
: This section specifies the hardware load balancer requirements, host computer hardware requirements, and operating system requirements for the enterprise deployment topology.

Reserving the Required IP Addresses for an Enterprise Deployment
: This section lists the set of IP addresses that you must obtain and reserve before installation and configuration.

Identifying and Obtaining Software Downloads for an Enterprise Deployment
: Before you begin installing and configuring the enterprise topology, you should locate and download the software distributions that you will need to implement the topology.

## 5.1 Hardware and Software Requirements for the Enterprise Deployment Topology

This section specifies the hardware load balancer requirements, host computer hardware requirements, and operating system requirements for the enterprise deployment topology.

This section includes the following sections.

Hardware Load Balancer Requirements
: This section lists the desired features of the external load balancer.

Host Computer Hardware Requirements
: This section provides information to help you procure host computers that are configured to support the enterprise deployment topologies.

Operating System Requirements for the Enterprise Deployment Topology
: This section provides details about the operating system requirements.

### 5.1.1 Hardware Load Balancer Requirements

This section lists the desired features of the external load balancer.

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

- Ability to load-balance traffic to a pool of real servers through a virtual host name: Clients access services using the virtual host name (instead of using actual host names). The load balancer can then load balance requests to the servers in the pool.
- Port translation configuration should be possible so that incoming requests on the virtual host name and port are directed to a different port on the backend servers.
- Monitoring of ports on the servers in the pool to determine availability of a service.
- Virtual servers and port configuration: Ability to configure virtual server names and ports on your external load balancer, and the virtual server names and ports must meet the following requirements:
  - The load balancer should allow configuration of multiple virtual servers. For each virtual server, the load balancer should allow configuration of traffic management on more than one port. For example, for Oracle HTTP Server in the web tier, the load balancer needs to be configured with a virtual server and ports for HTTP and HTTPS traffic.
  - The virtual server names must be associated with IP addresses and be part of your DNS. Clients must be able to access the external load balancer through the virtual server names.
- Ability to detect node failures and immediately stop routing traffic to the failed node.
- Fault-tolerant mode: It is highly recommended that you configure the load balancer to be in fault-tolerant mode.
- It is highly recommended that you configure the load balancer virtual server to return immediately to the calling client when the backend services to which it forwards traffic are unavailable. This is preferred over the client disconnecting on its own after a timeout based on the TCP/IP settings on the client machine.
- Sticky routing capability: Ability to maintain sticky connections to components. Examples of this include cookie-based persistence, IP-based persistence, and so on.
- The load balancer should be able to terminate SSL requests at the load balancer and forward traffic to the backend real servers using the equivalent non-SSL protocol (for example, HTTPS to HTTP).
- SSL acceleration (this feature is recommended, but not required for the enterprise topology).
- The ability to route TCP/IP requests; this is a requirement for Oracle SOA Suite for healthcare integration, which uses the Minimum Lower Layer Protocol (MLLP) over TCP.

## 5.1.2 Host Computer Hardware Requirements

This section provides information to help you procure host computers that are configured to support the enterprise deployment topologies.

It includes the following topics.

General Considerations for Enterprise Deployment Host Computers
: This section specifies the general considerations required for the enterprise deployment host computers.

Reviewing the Oracle Fusion Middleware System Requirements
: This section provides reference to the system requirements information to help you ensure that the environment meets the necessary minimum requirements.

Typical Memory, File Descriptors, and Processes Required for an Enterprise Deployment
: This section specifies the typical memory, number of file descriptors, and operating system processes and tasks details required for an enterprise deployment.

Typical Disk Space Requirements for an Enterprise Deployment
: This section specifies the disk space typically required for this enterprise deployment.

#### 5.1.2.1 General Considerations for Enterprise Deployment Host Computers

This section specifies the general considerations required for the enterprise deployment host computers.

Before you start the process of configuring an Oracle Fusion Middleware enterprise deployment, you must perform the appropriate capacity planning to determine the number of nodes, CPUs, and memory requirements for each node depending on the specific system's load as well as the throughput and response requirements. These requirements will vary for each application or custom Oracle WebCenter Portal system being used.

The information in this chapter provides general guidelines and information that will help you determine the host computer requirements. It does not replace the need to perform capacity planning for your specific production environment.

---

**Note:**

As you obtain and reserve the host computers in this section, note the host names and system characteristics in the Enterprise Deployment Workbook. You will use these addresses later when you enable the IP addresses on each host computer.

For more information, see Using the Enterprise Deployment Workbook

---

#### 5.1.2.2 Reviewing the Oracle Fusion Middleware System Requirements

This section provides reference to the system requirements information to help you ensure that the environment meets the necessary minimum requirements.

Review the *Oracle Fusion Middleware System Requirements and Specifications* to ensure that your environment meets the minimum installation requirements for the products you are installing.

The Requirements and Specifications document contains information about general Oracle Fusion Middleware hardware and software requirements, minimum disk space and memory requirements, database schema requirements, and required operating system libraries and packages.

It also provides some general guidelines for estimating the memory requirements for your Oracle Fusion Middleware deployment.

#### 5.1.2.3 Typical Memory, File Descriptors, and Processes Required for an Enterprise Deployment

This section specifies the typical memory, number of file descriptors, and operating system processes and tasks details required for an enterprise deployment.

The following table summarizes the memory, file descriptors, and processes required for the Administration Server and each of the Managed Servers computers in a typical Oracle WebCenter Portal enterprise deployment. These values are provided as an example only, but they can be used to estimate the minimum amount of memory required for an initial enterprise deployment.

The example in this topic reflects the minimum requirements for configuring the Managed Servers and other services required on WCPHOST1, as depicted in the reference topologies.

When you are procuring machines, use the information in the **Approximate Top Memory** column as a guide when determining the minimum physical memory each host computer should have available.

After you procure the host computer hardware and verify the operating system requirements, review the software configuration to be sure the operating system settings are configured to accommodate the number of open files listed in the **File Descriptors** column and the number processes listed in the **Operating System Processes and Tasks** column.

For more information, see Setting the Open File Limit and Number of Processes Settings on UNIX Systems.

| Managed Server, Utility, or Service | Approximate Top Memory | Number of File Descriptors | Operating System Processes and Tasks |
|---|---|---|---|
| Administration Server | 3.5 GB | 3500 | 165 |
| WLS_WSM | 3.0 GB | 2000 | 130 |
| WLS_Portal | 4.0 GB | 3100 | 240 |
| WLS_Portlet | 4.0 GB | 2200 | 180 |
| WLS_Collaboration | 3.5 GB | 1300 | 35 |
| WLST (connection to the Node Manager) | 1.5 GB | 910 | 20 |
| Configuration Wizard | 1.5 GB | 700 | 20 |
| Node Manager | 1.0 GB | 720 | 15 |
| TOTAL | 22.0 GB* | 14430 | 805 |

* Approximate total, with consideration for Operating System and other additional memory requirements.

#### 5.1.2.4 Typical Disk Space Requirements for an Enterprise Deployment

This section specifies the disk space typically required for this enterprise deployment.

For the latest disk space requirements for the Oracle Fusion Middleware 12*c* (12.2.1) products, including the Oracle WebCenter Portal products, review the *Oracle Fusion Middleware System Requirements and Specifications*.

In addition, the following table summarizes the disk space typically required for an Oracle WebCenter Portal enterprise deployment.

Use the this information and the information in Preparing the File System for an Enterprise Deployment to determine the disk space requirements required for your deployment.

| Server | Disk |
|---|---|
| Database | nXm<br>n = number of disks, at least 4 (striped as one disk)<br>m = size of the disk (minimum of 30 GB) |
| WEBHOST*n* | 10 GB |
| WCPHOST*n* | 10 GB* |

* For a shared storage Oracle home configuration, two installations suffice by making a total of 20 GB.

### 5.1.3 Operating System Requirements for the Enterprise Deployment Topology

This section provides details about the operating system requirements.

The Oracle Fusion Middleware software products and components described in this guide are certified on various operating systems and platforms, which are listed in the *Oracle Fusion Middleware System Requirements and Specifications*.

**Note:**

This guide focuses on the implementation of the enterprise deployment reference topology on Oracle Linux systems.

The topology can be implemented on any certified, supported operating system, but the examples in this guide typically show the commands and configuration steps as they should be performed using the bash shell on Oracle Linux.

## 5.2 Reserving the Required IP Addresses for an Enterprise Deployment

This section lists the set of IP addresses that you must obtain and reserve before installation and configuration.

Before you begin installing and configuring the enterprise topology, you must obtain and reserve a set of IP addresses:

- Physical IP (IP) addresses for each of the host computers you have procured for the topology
- A virtual IP (VIP) address for the Administration Server
- Additional VIP addresses for each Managed Server that is configured for Whole Server Migration

For Fusion Middleware 12*c* products that support Automatic Service Migration, VIPs for the Managed Servers are typically not necessary.

- A unique virtual host name to be mapped to each VIP.

You can then work with your network administrator to be sure these required VIPs are defined in your DNS server. (Alternatively, for non-production environments, you can use the /etc/hosts file to define these virtual hosts).

For more information, see the following topics.

What Is a Virtual IP (VIP) Address?
This section defines the virtual IP address and specifies its purpose.

Why Use Virtual Host Names and Virtual IP Addresses?
For an enterprise deployment, in particular, it is important that a set of VIPs--and the virtual host names to which they are mapped--are reserved and enabled on the corporate network.

Physical and Virtual IP Addresses Required by the Enterprise Topology
This section describes the physical IP (IP) and virtual IP (VIP) addresses required for the Administration Server and each of the Managed Servers in a typical Oracle WebCenter Portal enterprise deployment topology.

## 5.2.1 What Is a Virtual IP (VIP) Address?

This section defines the virtual IP address and specifies its purpose.

A virtual IP address is an unused IP Address that belongs to the same subnet as the host's primary IP address. It is assigned to a host manually. If a host computer fails, the virtual address can be assigned to a new host in the topology. For the purposes of this guide, we reference *virtual* IP addresses, which can be re-assigned from one host to another, and *physical* IP addresses, which are assigned permanently to hardware host computer.

## 5.2.2 Why Use Virtual Host Names and Virtual IP Addresses?

For an enterprise deployment, in particular, it is important that a set of VIPs--and the virtual host names to which they are mapped--are reserved and enabled on the corporate network.

Alternatively, host names can be resolved through appropriate `/etc/hosts` file propagated through the different nodes.

In the event of the failure of the host computer where the IP address is assigned, the IP address can be assigned to another host in the same subnet, so that the new host can take responsibility for running the Managed Servers assigned to it.

The reassignment of virtual IP address for the Administration Server must be performed manually, but the reassignment of virtual IP addresses for Managed Servers can be performed automatically using the Whole Server Migration feature of Oracle WebLogic Server.

Whether you should use Whole Server Migration or not depends upon the products you are deploying and whether they support Automatic Service Migration.

### 5.2.3 Physical and Virtual IP Addresses Required by the Enterprise Topology

This section describes the physical IP (IP) and virtual IP (VIP) addresses required for the Administration Server and each of the Managed Servers in a typical Oracle WebCenter Portal enterprise deployment topology.

Before you begin to install and configure the enterprise deployment, reserve a set of host names and IP addresses that correspond to the VIPs in Table 5-1.

You can assign any unique host name to the VIPs, but in this guide, we reference each VIP using the suggested host names in the table.

**Note:**

As you obtain and reserve the IP addresses and their corresponding virtual host names in this section, note the values of the IP addresses and host names in the Enterprise Deployment Workbook. You will use these addresses later when you enable the IP addresses on each host computer.

For more information, see Using the Enterprise Deployment Workbook

***Table 5-1 Summary of the Virtual IP Addresses Required for the Enterprise Deployment***

| Virtual IP | VIP Maps to... | Description |
|---|---|---|
| VIP1 | ADMINVHN | ADMINVHN is the virtual host name used as 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. |

## 5.3 Identifying and Obtaining Software Downloads for an Enterprise Deployment

Before you begin installing and configuring the enterprise topology, you should locate and download the software distributions that you will need to implement the topology.

The following table lists the downloads you will need to obtain.

For general information about how to obtain Oracle Fusion Middleware software, see Understanding and Obtaining Product Distributions in *Planning an Installation of Oracle Fusion Middleware*.

For more specific information about locating and downloading specific Oracle Fusion Middleware products, see the *Oracle Fusion Middleware Download, Installation, and Configuration Readme Files* on OTN.

| Distribution | Installer File Name | Description |
|---|---|---|
| Oracle Fusion Middleware 12*c* (12.2.1.1.0) Infrastructure | `fmw_12.2.1.1.0_infrastructure.jar` | Download this distribution to install the Oracle Fusion Middleware Infrastructure, which includes Oracle WebLogic Server and Java Required Files software required for Oracle Fusion Middleware products.<br>This distribution also installs the Repository Creation Utility (RCU), which in previous Oracle Fusion Middleware releases was packaged in its own distribution. |
| Oracle HTTP Server 12*c* (12.2.1.1.0) | `fmw_12.2.1.1.0_ohs_linux64.bin` | Download this distribution to install the Oracle HTTP Server software on the Web Tier. |
| Oracle Fusion Middleware 12*c* (12.2.1.1.0) WebCenter Portal | `fmw_12.2.1.1.0.wcportal_generic.jar` | Download this distribution to install the Oracle WebCenter Portal software. |
| Oracle Fusion Middleware 12*c* (12.2.1.1.0) WebCenter Content | `fmw_12.2.1.1.0_wccontent_generic.jar` | Download this distribution if you plan to add Oracle WebCenter Content to the WebCenter Portal topology. |
| Oracle Fusion Middleware 12*c* (12.2.1.1.0) SOA Suite and Business Process Management | `fmw_12.2.1.1.0_soa.jar` | Download this distribution if you plan to add Oracle SOA Suite to the WebCenter Portal topology. |

# 6

# Preparing the Load Balancer and Firewalls for an Enterprise Deployment

This chapter describes how to configure your network for an enterprise deployment.

Configuring Virtual Hosts on the Hardware Load Balancer
: This section explains how to configure the hardware load balancer for an enterprise deployment.

Configuring the Firewalls and Ports for an Enterprise Deployment
: As an administrator, it is important that you become familiar with the port numbers used by various Oracle Fusion Middleware products and services. This ensures that the same port number is not used by two services on the same host, and that the proper ports are open on the firewalls in the enterprise topology.

## 6.1 Configuring Virtual Hosts on the Hardware Load Balancer

This section explains how to configure the hardware load balancer for an enterprise deployment.

The following topics explain how to configure the hardware load balancer, provide the summary of the virtual servers required, and provide additional instructions for these virtual servers.

Overview of the Hardware Load Balancer Configuration

Typical Procedure for Configuring the Hardware Load Balancer

Summary of the Virtual Servers Required for an Enterprise Deployment

Additional Instructions for admin.example.com

Additional Instructions for wcp.example.com
: This section provides additional instructions for configuring the virtual server—wcp.example.com.

Additional Instructions for wcpinternal.example.com
: This section provides additional instructions for configuring the virtual server—wcpinternal.example.com.

### 6.1.1 Overview of the Hardware Load Balancer Configuration

As shown in the topology diagrams, you must configure the hardware load balancer to recognize and route requests to several virtual servers and associated ports for different types of network traffic and monitoring.

In the context of a load-balancing device, a virtual server is a construct that allows multiple physical servers to appear as one for load-balancing purposes. It is typically

represented by an IP address and a service, and it is used to distribute incoming client requests to the servers in the server pool.

The virtual servers should be configured to direct traffic to the appropriate host computers and ports for the various services available in the enterprise deployment.

In addition, you should configure the load balancer to monitor the host computers and ports for availability so that the traffic to a particular server 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.

Note that after you configure the load balancer, you can later configure the Web server instances in the Web tier to recognize a set of virtual hosts that use the same names as the virtual servers you defined for the load balancer. For each request coming from the hardware load balancer, the Web server can then route the request appropriately, based on the server name included in the header in the request. For more information, see Configuring Oracle HTTP Server for Administration and Oracle Web Services Manager.

## 6.1.2 Typical Procedure for Configuring the Hardware Load Balancer

The following procedure outlines the typical steps for configuring a hardware load balancer for an enterprise deployment.

Note that the actual procedures for configuring a specific load balancer will differ, depending on the specific type of load balancer. There may also be some differences depending on the type of protocol that is being load balanced. For example, TCP virtual servers and HTTP virtual servers use different types of monitors for their pools. Refer to the vendor-supplied documentation for actual steps.

1. Create a pool of servers. This pool contains a list of servers and the ports that are included in the load-balancing definition.

   For example, for load balancing between the Web hosts, create a pool of servers that would direct requests to hosts WEBHOST1 and WEBHOST2 on port 7777.

2. Create rules to determine whether or not a given host and service is available and assign it to the pool of servers described in Step 1.

3. Create the required virtual servers on the load balancer for the addresses and ports that receive requests for the applications.

   For a complete list of the virtual servers required for the enterprise deployment, see Summary of the Virtual Servers Required for an Enterprise Deployment.

   When you define each virtual server on the load balancer, consider the following:

   a. If your load balancer supports it, specify whether or not the virtual server is available internally, externally or both. Ensure that internal addresses are only resolvable from inside the network.

   b. Configure SSL Termination, if applicable, for the virtual server.

   c. Assign the pool of servers created in Step 1 to the virtual server.

## 6.1.3 Summary of the Virtual Servers Required for an Enterprise Deployment

This section provides the details of the virtual servers required for an enterprise deployment.

The following table provides a list of the virtual servers you must define on the hardware load balancer for the Oracle WebCenter Portal enterprise topology.

| Virtual Host | Server Pool | Protocol | SSL Termination? | External? |
|---|---|---|---|---|
| admin.example.com:80 | WEBHOST1.example.com:7777<br>WEBHOST2.example.com:7777 | HTTP | No | No |
| wcp.example.com:443 | WEBHOST1.example.com:7777<br>WEBHOST2.example.com:7777 | HTTPS | Yes | Yes |
| wcpinternal.example.com:80 | WEBHOST1.example.com:7777<br>WEBHOST2.example.com:7777 | HTTP | No | No |
| wcpinternal.example.com:6300 | WCCHOST1.example.com:4444<br>WCCHOST2.example.com:4444 | TCP | No | No |

### 6.1.4 Additional Instructions for admin.example.com

This section provides the additional instructions required for the virtual server—admin.example.com.

When you configure this virtual server on the hardware load balancer:

- Enable address and port translation.
- Enable reset of connections when services or hosts are down.

### 6.1.5 Additional Instructions for wcp.example.com

This section provides additional instructions for configuring the virtual server—wcp.example.com.

When you configure this virtual server on the hardware load balancer:

- Use port 80 and port 443. Any request that goes to port 80 (non-ssl protocol) should be redirected to port 443 (ssl protocol).
- Specify HTTP as the protocol.
- Enable address and port translation.
- Enable reset of connections when services and/or nodes are down.
- Create rules to filter out access to `/console` and `/em` on this virtual server.

  These context strings direct requests to the Oracle WebLogic Server Administration Console and to the Oracle Enterprise Manager Fusion Middleware Control and should be used only when accessing the system from `admin.example.com`.

### 6.1.6 Additional Instructions for wcpinternal.example.com

This section provides additional instructions for configuring the virtual server—wcpinternal.example.com.

This virtual server is used for internal invocations of WebCenter Portal and WebCenter Content services. This URL is not exposed to the Internet and is accessible only from the intranet. The incoming traffic from clients is not SSL enabled. Two

virtual servers are configured at the hardware load balancer using this address with different ports.

This address is used for both HTTP and Remote Intradoc Client (RIDC) traffic:

- HTTP connections are received at the hardware load balancer on port 80 and forwarded to the WEBHOST servers on the OHS default port 7777.
- RIDC TCP connections are received at the hardware load balancer on port 6300 and forwarded to the WCCHOST servers on the RIDC default port 4444.

> **Note:**
>
> It is recommended to use a unique port for the front-end configuration versus simply receiving and forwarding on the RIDC service port number (for example, 4444).

Two server pools are configured at the hardware load balancer to support this topology:

1. Web servers; containing: WEBHOST1:7777 and WEBHOST2:7777
2. RIDC servers; containing: WCCHOST1:4444 and WCCHOST2:4444

The RIDC traffic uses port 6300 on the load balancer (6300 is mainly for masking), but the traffic ultimately routes to the RIDC port (4444) on the WebCenter hosts.

When you configure this virtual server on the hardware load balancer:

- Enable address and port translation.
- Enable reset of connections when services or nodes are down.
- As with the `wcp.example.com`, create rules to filter out access to `/console` and `/em` on this virtual server.

## 6.2 Configuring the Firewalls and Ports for an Enterprise Deployment

As an administrator, it is important that you become familiar with the port numbers used by various Oracle Fusion Middleware products and services. This ensures that the same port number is not used by two services on the same host, and that the proper ports are open on the firewalls in the enterprise topology.

The following tables lists the ports that you must open on the firewalls in the topology.

Firewall notation:

- FW1 refers to the outermost firewall.
- FW2 refers to the firewall between the web tier and the application tier.
- FW3 refers to the firewall between the application tier and the data tier.

### Firewall Ports Common to All Fusion Middleware Enterprise Deployments

| 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 the size and type of HTML content. |
| Browser request | FW0 | 443 | HTTPS / Load Balancer | Inbound | Timeout depends on the size and type of HTML content. |
| Browser request | FW1 | 80 | HTTPS / Load Balancer | Outbound (for intranet clients) | Timeout depends on the size and type of HTML content. |
| Browser request | FW1 | 443 | HTTPS / Load Balancer | Outbound (for intranet clients) | Timeout depends on the size and type of HTML content. |
| Callbacks and Outbound invocations | FW1 | 80 | HTTPS / Load Balancer | Outbound | Timeout depends on the size and type of HTML content. |
| Callbacks and Outbound invocations | FW1 | 443 | HTTPS / Load Balancer | Outbound | Timeout depends on the size and type of HTML content. |
| Load balancer to Oracle HTTP Server | n/a | 7777 | HTTP | n/a | n/a |
| 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 | OHS Admin Port (7779) | TCP and HTTP, respectively | Outbound | Set the timeout to a short period (5-10 seconds). |

| Type | Firewall | Port and Port Range | Protocol / Application | Inbound / Outbound | Other Considerations and Timeout Guidelines |
|---|---|---|---|---|---|
| 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 Enterprise Manager<br>t3 | Both | You should tune this timeout based on the type of access to the admin console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier). |
| Database access | FW2 | 1521 | SQL*Net | Both | Timeout depends on database content and on the type of process model used for SOA. |
| Coherence for deployment | n/a | 8088<br>Range: 8000 - 8090 | | n/a | n/a |
| Oracle Unified Directory access | FW2 | 389<br>636 (SSL) | LDAP or LDAP/ssl | Inbound | You should tune the directory server's parameters based on load balancer, and not the other way around. |

| Type | Firewall | Port and Port Range | Protocol / Application | Inbound / Outbound | Other Considerations and Timeout Guidelines |
|---|---|---|---|---|---|
| Oracle Notification Server (ONS) | FW2 | 6200 | ONS | Both | Required for Gridlink. An ONS server runs on each database server. |

### Firewall Ports Specific to Oracle WebCenter Portal Enterprise Deployments

| Type | Firewall | Port and Port Range | Protocol / Application | Inbound / Outbound | Other Considerations and Timeout Guidelines |
|---|---|---|---|---|---|
| WSM-PM access | FW1 | 7010<br>Range: 7010 - 7999 | HTTP / WLS_WSM-PM*n* | Inbound | Set the timeout to 60 seconds. |
| Portal Server access | FW1 | 9001 | HTTP / WLS_Portal*n* | Inbound | Set the timeout to a short period (5–10 seconds). |
| Portlet Server Access | FW1 | 9002 | HTTP / WLS_Portlet*n* | Inbound | Set the timeout to a short period (5-10 seconds). |
| Collaboration Server Access | FW1 | 9003 | HTTP / WLS_Collab*n* | Inbound | Set the timeout to a short period (5-10 seconds). |
| RIDC API requests | FW1 | 6300 | TCP/ WLS_WCC*n* | Inbound | n/a |

# 7

# Preparing the File System for an Enterprise Deployment

Involves understanding the requirements for local and shared storage, as well as the terminology used to reference important directories and file locations during the installation and configuration of the enterprise topology.

This chapter describes how to prepare the file system for an Oracle Fusion Middleware enterprise deployment.



## 7.1 Overview of Preparing the File System for an Enterprise Deployment

This section provides an overview of the process of preparing the file system for an enterprise deployment.

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

Use this chapter as a reference to help understand the directory variables used in the installation and configuration procedures.

Other directory layouts are possible and supported, but the model adopted in this guide was designed for maximum availability, providing both the best isolation of components and symmetry in the configuration and facilitating backup and disaster recovery. The rest of the document uses this directory structure and directory terminology.

## 7.2 Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment

This section provides reference to the shared storage recommendations when installing and configuring an enterprise deployment.

Before you implement the detailed recommendations in this chapter, be sure to review the recommendations and general information about using shared storage in the *High Availability Guide*.

The recommendations in this chapter are based on the concepts and guidelines described in the *High Availability Guide*.

Table 7-1 lists the key sections you should review and how those concepts apply to an enterprise deployment.

***Table 7-1 Shared Storage Resources in the High Availability Guide***

| Section in *High Availability Guide* | Importance to an Enterprise Deployment |
|---|---|
| Shared Storage Prerequisites | Describes guidelines for disk format and the requirements for hardware devices that are optimized for shared storage. |
| Using Shared Storage for Binary (Oracle Home) Directories | Describes your options for storing the Oracle home on a shared storage device that is available to multiple hosts.<br>For the purposes of the enterprise deployment, Oracle recommends using redundant Oracle homes on separate storage volumes.<br>If a separate volume is not available, a separate partition on the shared disk should be used to provide redundant Oracle homes to application tier hosts. |
| Using Shared Storage for Domain Configuration Files | Describes the concept of creating separate domain homes for the Administration Server and the Managed Servers in the domain.<br>For an enterprise deployment, the Administration Server domain home location is referenced by the *ASERVER_HOME* variable. |
| Shared Storage Requirements for JMS Stores and JTA Logs | Provides instructions for setting the location of the transaction logs and JMS stores for an enterprise deployment. |

## 7.3 Understanding the Recommended Directory Structure for an Enterprise Deployment

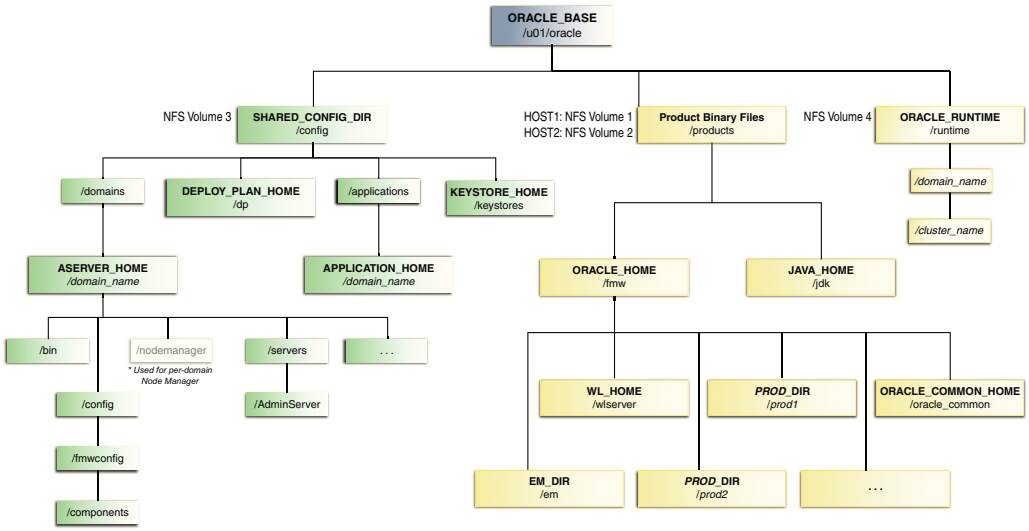
The diagrams in this section show the recommended directory structure for a typical Oracle Fusion Middleware enterprise deployment.

The directories shown in the diagrams contain binary files that are installed on disk by the Oracle Fusion Middleware installers, domain-specific files generated via the domain configuration process, as well as domain configuration files that are propagated to the various host computers via the Oracle WebLogic Server `pack` and `unpack` commands:

- Figure 7-1 shows the resulting directory structure on the shared storage device after you have installed and configured a typical Oracle Fusion Middleware enterprise deployment. The shared storage directories are accessible by the application tier host computers.
- Figure 7-2 shows the resulting directory structure on the local storage device for a typical application tier host after you have installed and configured an Oracle Fusion Middleware enterprise deployment. The Managed Servers in particular are stored on the local storage device for the application tier host computers.
- Figure 7-3 shows the resulting directory structure on the local storage device for a typical Web tier host after you have installed and configured an Oracle Fusion Middleware enterprise deployment. Note that the software binaries (in the Oracle home) are installed on the local storage device for each Web tier host.

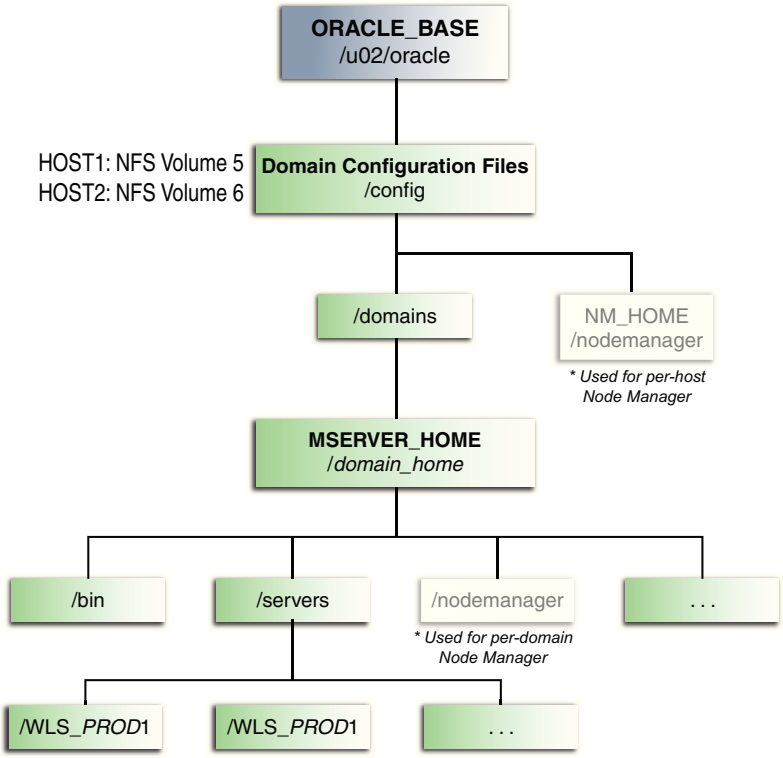
Where applicable, the diagrams also include the standard variables used to reference the directory locations in the installation and configuration procedures in this guide.

***Figure 7-1 Recommended Shared Storage Directory Structure for an Enterprise Deployment***



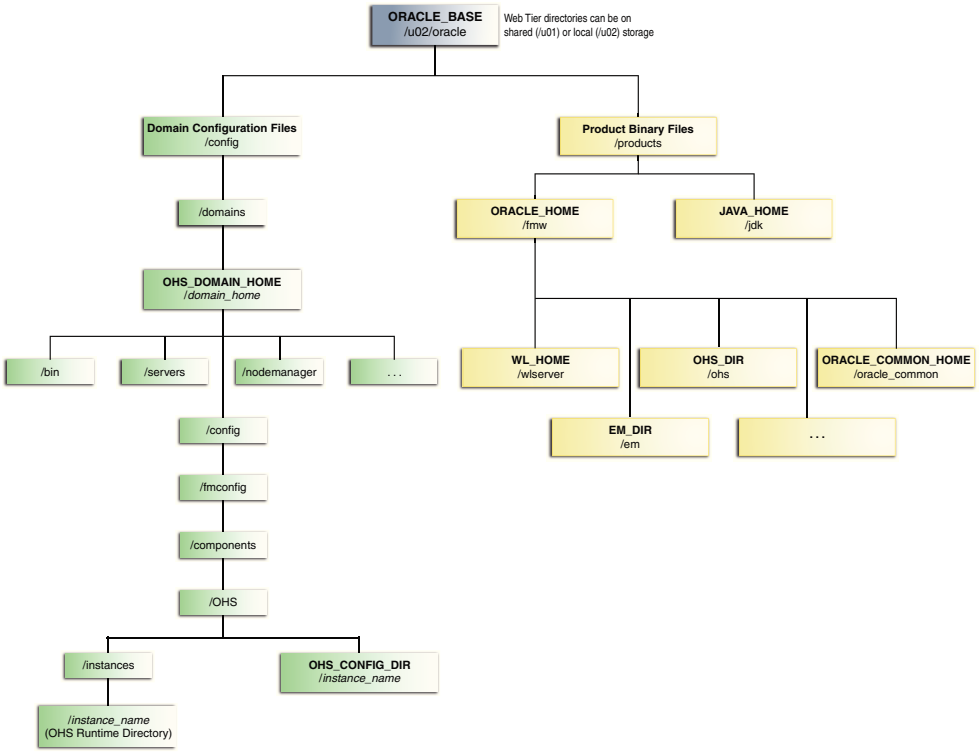

* For more information, see About the Node Manager Configuration in a Typical Enterprise Deployment.

***Figure 7-2 Recommended Local Storage Directory Structure for an Application Tier Host Computer in an Enterprise Deployment***




* For more information, see About the Node Manager Configuration in a Typical Enterprise Deployment.

***Figure 7-3 Recommended Local Storage Directory Structure for a Web Tier Host Computer in an Enterprise Deployment***




## 7.4 File System and Directory Variables Used in This Guide

This section lists and describes the file system and directory variables used throughout this guide.

Table 7-2 lists the file system directories and the directory variables used to reference the directories on the Application tier. Table 7-3 lists the file system directories and variables used to reference the directories on the Web tier.

For additional information about mounting these directories when you are using shared storage, see About Creating and Mounting the Directories for an Enterprise Deployment.

Throughout this guide, the instructions for installing and configuring the topology refer to the directory locations using the variables shown here.

You can also define operating system variables for each of the directories listed in this section. If you define system variables for the particular UNIX shell you are using, you can then use the variables as they are used in this document, without having to map the variables to the actual values for your environment.

---

**Note:**

As you configure your storage devices to accommodate the recommended directory structure, note the actual directory paths in the Enterprise Deployment Workbook. You will use these addresses later when you enable the IP addresses on each host computer.

For more information, see Using the Enterprise Deployment Workbook..

---

***Table 7-2 Sample Values for Key Directory Variables on the Application Tier***

| Directory Variable | Description | Sample Value on the Application Tier |
|---|---|---|
| *ORACLE_BASE* | The base directory, under which Oracle products are installed. | `/u01/oracle` |
| *ORACLE_HOME* | The read-only location for the product binaries. For the application tier host computers, it is stored on shared disk.<br>The Oracle home is created when you install the Oracle Fusion Middleware Infrastructure software.<br>You can then install additional Oracle Fusion Middleware products into the same Oracle home. | `/u01/oracle/products/fmw` |
| *ORACLE_COMMON_HOME* | The directory within the Oracle Fusion Middleware Oracle home where common utilities, libraries, and other common Oracle Fusion Middleware products are stored. | `/u01/oracle/products/fmw/oracle_common` |
| *WL_HOME* | The directory within the Oracle home where the Oracle WebLogic Server software binaries are stored. | `/u01/oracle/products/fmw/wlserver` |
| *PROD_DIR* | Individual product directories for each Oracle Fusion Middleware product you install. | `/u01/oracle/products/fmw/`*`prod_dir`*<br>The product can be `soa`, `wcc`, `bi`, or another value, depending on your enterprise deployment. |
| *EM_DIR* | The product directory used to store the Oracle Enterprise Manager Fusion Middleware Control software binaries. | `/u01/oracle/products/fmw/em` |
| *JAVA_HOME* | The location where you install the supported Java Development Kit (JDK). | `/u01/oracle/products/jdk` |
| *SHARED_CONFIG_DIR* | The shared parent directory for shared environment configuration files, including domain configuration, keystores, runtime artifacts, and application deployments | `/u01/oracle/config` |
| *ASERVER_HOME* | The Administration Server domain home, which is installed on shared disk. | `/u01/oracle/config/domains/`*`domain_name`*<br>In this example, replace domain_name with the name of the WebLogic Server domain. |
| *MSERVER_HOME* | The Managed Server domain home, which is created via the unpack command on the local disk of each application tier host. | `/u02/oracle/config/domains/`*`domain_name`* |

***Table 7-2 (Cont.) Sample Values for Key Directory Variables on the Application Tier***

| Directory Variable | Description | Sample Value on the Application Tier |
|---|---|---|
| *APPLICATION_HOME* | The Application home directory, which is installed on shared disk, so the directory is accessible by all the application tier host computers. | `/u01/oracle/config/applications/domain_name` |
| *ORACLE_RUNTIME* | This directory contains the Oracle runtime artifacts, such as the JMS logs and TLogs.<br>Typically, you mount this directory as a separate shared file system, which is accessible by all hosts in the domain.<br>When you run the Configuration Wizard or perform post-configuration tasks, and you identify the location of JMS stores or tlogs persistent stores, then you can use this directory, qualified with the name of the domain, the name of the cluster, and the purpose of the directory.<br>For example:<br>`ORACLE_RUNTIME/cluster_name/jms` | `/u01/oracle/runtime/` |
| *NM_HOME* | The directory used by the Per Machine Node Manager start script and configuration files.<br>**Note:** This directory is necessary only if you are using a Per Machine Node Manager configuration.<br>For more information, see About the Node Manager Configuration in a Typical Enterprise Deployment. | `/u02/oracle/config/node_manager` |
| *DEPLOY_PLAN_HOME* | The deployment plan directory, which is used as the default location for application deployment plans.<br>**Note:** This directory is required only when you are deploying custom applications to the application tier. | `/u01/oracle/config/dp` |

***Table 7-2 (Cont.) Sample Values for Key Directory Variables on the Application Tier***

| Directory Variable | Description | Sample Value on the Application Tier |
|---|---|---|
| *KEYSTORE_HOME* | The shared location for custom certificates and keystores. | `/u01/oracle/config/keystores` |

***Table 7-3 Sample Values for Key Directory Variables on the Web Tier***

| Directory Variable | Description | Sample Value on the Web Tier |
|---|---|---|
| *OHS_ORACLE_HOME* | The read-only location for the Oracle HTTP Server product binaries. For the Web tier host computers, this directory is stored on local disk.<br>The Oracle home is created when you install the Oracle HTTP Server software. | `/u02/oracle/products/fmw` |
| *ORACLE_COMMON_HOME* | The directory within the Oracle HTTP Server Oracle home where common utilities, libraries, and other common Oracle Fusion Middleware products are stored. | `/u02/oracle/products/fmw/oracle_common` |
| *WL_HOME* | The directory within the Oracle home where the Oracle WebLogic Server software binaries are stored. | `/u02/oracle/products/fmw/wlserver` |
| *PROD_DIR* | Individual product directories for each Oracle Fusion Middleware product you install. | `/u02/oracle/products/fmw/ohs` |
| *JAVA_HOME* | The location where you install the supported Java Development Kit (JDK). | `/u02/oracle/products/jdk` |
| *OHS_DOMAIN_HOME* | The Domain home for the standalone Oracle HTTP Server domain, which is created when you install Oracle HTTP Server on the local disk of each Web tier host. | `/u02/oracle/config/domains/`*`domain_name`* |
| *OHS_CONFIG_DIR* | This is the location where you edit the Oracle HTTP Server configuration files (for example, `httpd.conf` and `moduleconf/*.conf`) on each Web host.<br>Note this directory is also referred to as the OHS Staging Directory. Changes made here are later propagated to the OHS Runtime Directory.<br>For more information, see "Staging and Run-time Configuration Directories" in the *Administrator's Guide for Oracle HTTP Server*. | `/u02/oracle/config/domains/`*`domain_name`*`/config/fmwconfig/components/OHS/`*`instance_name`* |

## 7.5 About Creating and Mounting the Directories for an Enterprise Deployment

This section lists the best practices to be followed when creating or mounting the top-level directories in an enterprise deployment.

When creating or mounting the top-level directories, note the following best practices:

- For the application tier, install the Oracle home (which contains the software binaries) on a second shared storage volume or second partition that is mounted to WCPHOST2. Be sure the directory path to the binaries on WCPHOST2 is identical to the directory path on WCPHOST1.

  For example:

  ```
  /u01/oracle/products/fmw/
  ```

  For more information, see Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment.

- This enterprise deployment guide assumes that the Oracle Web tier software will be installed on a local disk.

  The Web tier installation is typically performed on local storage to the WEBHOST nodes. When using shared storage, you can install the Oracle Web tier binaries (and create the Oracle HTTP Server instances) on shared disk. However, if you do so, then the shared disk *must* be separate from the shared disk used for the application tier, and you must consider the appropriate security restrictions for access to the storage device across tiers.

  As with the application tier servers (WCPHOST1 and WCPHOST2), use the same directory path on both computers.

  For example:

  ```
  /u02/oracle/products/fmw/
  ```

## 7.6 Summary of the Shared Storage Volumes in an Enterprise Deployment

This section provides a summary of the shared storage volumes required for an enterprise deployment.

The following table summarizes the shared volumes and their purpose in a typical Oracle Fusion Middleware enterprise deployment.

For more information, see Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment.

| Volume in Shared Storage | Mounted to Host | Mount Directories | Description and Purpose |
|---|---|---|---|
| NFS Volume 1 | WCPHOST1<br>WCCHOST1 | `/u01/oracle/products/` | Local storage for the product binaries to be used by WCPHOST1; this is where the Oracle home directory and product directories are installed. |
| NFS Volume 2 | WCPHOST2<br>WCCHOST2 | `/u01/oracle/products/` | Local storage for the product binaries to be used by WCPHOST2; this is where the Oracle home directory and product directories are installed. |

| Volume in Shared Storage | Mounted to Host | Mount Directories | Description and Purpose |
|---|---|---|---|
| NFS Volume 3 | WCPHOST1 WCPHOST2<br>WCCHOST1<br>WCCHOST2 | `/u01/oracle/config/` | Administration Server domain configuration, mounted to all hosts; used initially by WCPHOST1, but can be failed over to any host. |
| NFS Volume 4 | WCPHOST1 WCPHOST2<br>WCCHOST1<br>WCCHOST2 | `/u01/oracle/runtime/` | The runtime artifacts directory, mounted to all hosts, contains runtime artifacts such as JMS logs, blogs, and any cluster-dependent shared files needed. |
| NFS Volume 5 | WCPHOST1 | `/u02/oracle/config/` | Local storage for the Managed Server domain directory to be used by WCPHOST1, if the private Managed Server domain directory resides on shared storage. |
| NFS Volume 6 | WCPHOST2 | `/u02/oracle/config/` | Local storage for the Managed Server domain directory to be used by WCPHOST2, if the private Managed Server domain directory resides on shared storage. |
| NFS Volume 7 | WEBHOST1 | `/u02/oracle/` | Local storage for the Oracle HTTP Server software binaries (Oracle home) and domain configuration files used by WEBHOST1, if the private Managed Server domain directory resides on shared storage. |
| NFS Volume 8 | WEBHOST2 | `/u02/oracle/` | Local storage for the Oracle HTTP Server software binaries (Oracle home) and domain configuration files used by WEBHOST2, if the private Managed Server domain directory resides on shared storage. |

| Volume in Shared Storage | Mounted to Host | Mount Directories | Description and Purpose |
|---|---|---|---|
| NFS Volume 9 | WCCHOST1 | `/u02/oracle/config/` | Local storage for the Managed Server domain directory to be used by WCCHOST1, if the private Managed Server domain directory resides on shared storage. |
| NFS Volume 10 | WCCHOST2 | `/u02/oracle/config/` | Local storage for the Managed Server domain directory to be used by WCCHOST2, if the private Managed Server domain directory resides on shared storage. |

# 8

# Preparing the Host Computers for an Enterprise Deployment

It explains how to mount the required shared storage systems to the host and how to enable the required virtual IP addresses on each host.

This chapter describes the tasks you must perform from each computer or server that will be hosting the enterprise deployment.

Verifying the Minimum Hardware Requirements for Each Host
: This section provides information about the minimum hardware requirements for each host.

Verifying Linux Operating System Requirements
: Review this section for typical Linux operating system settings for an enterprise deployment.

Configuring Operating System Users and Groups
: The lists in this section show the users and groups to define on each of the computers that will host the enterprise deployment.

Enabling Unicode Support
: This section provides information about enabling Unicode support.

Mounting the Required Shared File Systems on Each Host
: This section provides information about mounting the required shared file systems on each host.

Enabling the Required Virtual IP Addresses on Each Host
: This section provides instruction to enable the required virtual IP addresses on each host.

## 8.1 Verifying the Minimum Hardware Requirements for Each Host

This section provides information about the minimum hardware requirements for each host.

After you have procured the required hardware for the enterprise deployment, log in to each host computer and verify the system requirements listed in Hardware and Software Requirements for the Enterprise Deployment Topology.

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 storage and shared storage configured as described in Preparing the File System for an Enterprise Deployment.

Allow sufficient swap and temporary space; specifically:

- **Swap Space**–The system must have at least 500 MB.

- **Temporary Space**–There must be a minimum of 500 MB of free space in `/tmp`.

## 8.2 Verifying Linux Operating System Requirements

Review this section for typical Linux operating system settings for an enterprise deployment.

To ensure the host computers meet the minimum operating system requirements, be sure you have installed a certified operating system and that you have applied all the necessary patches for the operating system.

In addition, review the following sections for typical Linux operating system settings for an enterprise deployment.

Setting Linux Kernel Parameters

Setting the Open File Limit and Number of Processes Settings on UNIX Systems

Verifying IP Addresses and Host Names in DNS or hosts File

### 8.2.1 Setting Linux Kernel Parameters

The kernel-parameter and shell-limit values shown below are recommended values only. Oracle recommends that you tune these values to optimize the performance of the system. See your operating system documentation for more information about tuning kernel parameters.

Kernel parameters must be set to a minimum of those in Table on all nodes in the topology.

The values in the following table are the current Linux recommendations. For the latest recommendations for Linux and other operating systems, see *Oracle Fusion Middleware System Requirements and Specifications*.

If you are deploying a database onto the host, you might need to modify additional kernel parameters. Refer to the 12c (12.2.1) *Oracle Grid Infrastructure Installation Guide* for your platform.

***Table 8-1 UNIX Kernel Parameters***

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

To set these parameters:

1. Log in as `root` and add or amend the entries in the file `/etc/sysctl.conf`.
2. Save the file.
3. Activate the changes by issuing the command:

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

## 8.2.2 Setting the Open File Limit and Number of Processes Settings on UNIX Systems

On UNIX operating systems, the `Open File Limit` is an important system setting, which can affect the overall performance of the software running on the host computer.

For guidance on setting the `Open File Limit` for an Oracle Fusion Middleware enterprise deployment, see Host Computer Hardware Requirements.

---

**Note:**

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

---

For more information, see the following sections.

Viewing the Number of Currently Open Files

Setting the Operating System Open File and Processes Limits

### 8.2.2.1 Viewing the Number of Currently Open Files

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 following commands.

**C shell**:

```
limit descriptors
```

**Bash**:

```
ulimit -n
```

### 8.2.2.2 Setting the Operating System Open File and Processes Limits

To change the Open File Limit values:

1. Log in as `root` and edit the following file:

   `/etc/security/limits.conf`

2. Add the following lines to the `limits.conf` file. (The values shown here are for example only):

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

   The `nofiles` values represent the open file limit; the `nproc` values represent the number of processes limit.

3. Save the changes, and close the `limits.conf` file.

4. Reboot the host computer.

### 8.2.3 Verifying IP Addresses and Host Names in DNS or hosts File

Before you begin the installation of the Oracle software, ensure that the IP address, fully qualified host name, and the short name of the host are all registered with your DNS server. Alternatively, you can use the local `hosts` file and add an entry similar to the following:

```
IP_Address Fully_Qualified_Name Short_Name
```

For example:

```
10.229.188.205  host1.example.com  host1
```

## 8.3 Configuring Operating System Users and Groups

The lists in this section show the users and groups to define on each of the computers that will host the enterprise deployment.

**Groups**

You must create the following groups on each node.

- `oinstall`
- `dba`

**Users**

You must create the following user on each node.

- `nobody`–An unprivileged user.
- `oracle`–The owner of the Oracle software. You may use a different name. The primary group for this account must be `oinstall`. The account must also be in the `dba` group.

---

**Note:**

- The group `oinstall` must have write privileges to all the file systems on shared and local storage that are used by the Oracle software.
- Each group must have the same Group ID on every node.
- Each user must have the same User ID on every node.

---

## 8.4 Enabling Unicode Support

This section provides information about 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 WebCenter Portal technologies, for example, are based on Unicode.

If the operating system is configured to use a non-UTF-8 encoding, Oracle WebCenter Portal 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.

## 8.5 Mounting the Required Shared File Systems on Each Host

This section provides information about mounting the required shared file systems on each host.

The shared storage configured, as described in Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment, must be available on the hosts that use it.

In an enterprise deployment, it is assumed that you have a hardware storage filer, which is available and connected to each of the host computers you have procured for the deployment.

You must mount the shared storage to all servers that require access.

Each host must have appropriate privileges set within the Network Attached Storage (NAS) or Storage Area Network (SAN) so that it can write to the shared storage.

Follow the best practices of your organization for mounting shared storage. This section provides an example of how to do this on Linux using NFS storage.

You must create and mount shared storage locations so that WCPHOST1 and WCPHOST2 can see the same location if it is a binary installation in two separate volumes.

For more information, see Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment.

You use the following command to mount shared storage from a NAS storage device to a Linux host. If you are using a different type of storage device or operating system, refer to your manufacturer documentation for information about how to do this.

---

**Note:**

The user account used to create a shared storage file system owns and has read, write, and execute privileges for those files. Other users in the operating system group can read and execute the files, but they do not have write privileges.

For more information about installation and configuration privileges, see "Selecting an Installation User" in the *Oracle Fusion Middleware Installation Planning Guide*.

---

In the following example, `nasfiler` represents the shared storage filer. Also note that these are examples only. Typically, the mounting of these shared storage locations should be done using the `/etc/fstabs` file on UNIX systems, so that the mounting of these devices survives a reboot. Refer to your operating system documentation for more information.

1. Create the mount directories on WCPHOST1, as described in Summary of the Shared Storage Volumes in an Enterprise Deployment, and then mount the shared storage. For example:

   ```
   mount -t nfs nasfiler:VOL1/oracle/products/ /u01/oracle/products/
   ```

2. Repeat the procedure on WCPHOST2 using VOL2.

### Validating the Shared Storage Configuration

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

For example:

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

Verify that the owner and permissions are correct:

```
$ ls -l testfile
```

Then remove the file:

```
$ rm testfile
```

---

**Note:**

The shared storage can be a NAS or SAN device. The following example illustrates creating storage for a NAS device from WCPHOST1. The options may differ depending on the specific storage device.

```
mount -t nfs -o
rw,bg,hard,nointr,tcp,vers=3,timeo=300,rsize=32768,wsize=32768 nasfiler:VOL1/
Oracle /u01/oracle
```

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

---

## 8.6 Enabling the Required Virtual IP Addresses on Each Host

This section provides instruction to enable the required virtual IP addresses on each host.

To prepare each host for the enterprise deployment, you must enable the virtual IP (VIP) addresses described in Reserving the Required IP Addresses for an Enterprise Deployment.

It is assumed that you have already reserved the VIP addresses and host names and that they have been enabled by your network administrator. You can then enable the VIPs on the appropriate host.

Note that the virtual IP addresses used for the enterprise topology are not persisted because they are managed by Whole Server Migration (for selected Managed Servers and clusters) or by manual failover (for the Administration Server).

---

**Note:**

For WebCenter Portal and Content, there is only one VIP required to be enabled on WCPHOST1, for the manual fail-over of the Administration Server.

---

To enable the VIP addresses on each host, run the following commands as `root`:

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

where *interface* is eth0, 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 using the ping command from another node, for example:

```
/bin/ping 100.200.140.206
```

# 9

# Preparing the Database for an Enterprise Deployment

This chapter describes procedures for preparing your database for an Oracle WebCenter Portal enterprise deployment.

This chapter provides information about the database requirements, creating database services and about the database backup strategies.

Overview of Preparing the Database for an Enterprise Deployment
: This section provides information about how to configure a supported database as part of an Oracle Fusion Middleware enterprise deployment.

About Database Requirements
: Check that the database meets the requirements described in these sections.

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.

Using SecureFiles for Large Objects (LOBs) in an Oracle Database
: Beginning with Oracle Database 11g Release 1, Oracle introduced SecureFiles, a new LOB storage architecture. Oracle recommends using SecureFiles for the Oracle Fusion Middleware schemas, in particular for the Oracle SOA Suite schemas.

About Database Backup Strategies
: This section provides brief information about the necessity of database backup strategies.

## 9.1 Overview of Preparing the Database for an Enterprise Deployment

This section provides information about how to configure a supported database as part of an Oracle Fusion Middleware enterprise deployment.

Most Oracle Fusion Middleware products require a specific set of schemas that must be installed in a supported database. The schemas are installed using the Oracle Fusion Middleware Repository Creation Utility (RCU).

In an enterprise deployment, Oracle recommends a highly available Real Application Clusters (Oracle RAC) database for the Oracle Fusion Middleware product schemas.

## 9.2 About Database Requirements

Check that the database meets the requirements described in these sections.

Supported Database Versions

## 9.2.1 Supported Database Versions

Use the following information to verify what databases are supported by each Oracle Fusion Middleware release and which version of the Oracle database you are currently running:

- For a list of all certified databases, refer to *Oracle Fusion Middleware Supported System Configurations*.
- To check the release of your database, query the `PRODUCT_COMPONENT_VERSION` view:

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

Oracle Fusion Middleware requires that the database supports the AL32UTF8 character set. Check the database documentation for information on choosing a character set for the database.

For enterprise deployments, Oracle recommends using GridLink data sources to connect to Oracle RAC databases.

---

**Note:**

For more information about using GridLink data sources and SCAN, see "Using Active GridLink Data Sources" in *Administering JDBC Data Sources for Oracle WebLogic Server*.

---

## 9.2.2 Additional Database Software Requirements

In the enterprise topology, there are two database host computers in the data tier that host the two instances of the RAC database. We refer to these hosts as DBHOST1 and DBHOST2.

Before you install or configure the enterprise topology, you must be sure the following software is installed and available on DBHOST1 and DBHOST2:

- **Oracle Clusterware**

  For more information, see the *Oracle Grid Infrastructure Installation Guide for Linux*.

- **Oracle Real Application Clusters**

  For more information, see the *Oracle Real Application Clusters Installation Guide for Linux and UNIX*.

- **Time synchronization between Oracle RAC database instances**

  The clocks of the database instances must be in sync if they are used by servers in a Fusion Middleware cluster configured with server migration.

- **Automatic Storage Management** (optional)

  For more information, see the *Oracle Automatic Storage Management Administrator's Guide*.

### 9.2.3 Installing and Validating Oracle Text

Before you install or configure the WebCenter Content enterprise topology, you must be sure that Oracle Text is installed and available on DBHOST1 and DBHOST2.

For more information on installing Oracle Text, see the *Oracle Database Installation Guide for Linux*.

To make sure that the database used for WebCenter Content installation has Oracle Text enabled, run the following command:

```
SQL> select comp_name, status, substr(version,1,10) as version from dba_registry
where comp_id = 'CONTEXT';

COMP_NAME STATUS VERSION
----------- ------- -------
Oracle Text VALID 12.1.0.1.0
```

## 9.3 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.

---

**Note:**

The instructions in this section are for the Oracle Database 12*c* (12.1) release. If you are using another supported database, refer to the appropriate documentation library for more up-to-date and release-specific information.

---

For more information about connecting to Oracle databases using services, see "Overview of Using Dynamic Database Services to Connect to Oracle Databases" in the *Real Application Clusters Administration and Deployment Guide*.

In addition, the database service should be different from the default database service. For complete instructions on creating and managing database services for an Oracle Database 12*c* database, see "Overview of Automatic Workload Management with Dynamic Database Services" in the *Real Application Clusters Administration and Deployment Guide*.

Run-time connection load balancing requires configuring Oracle RAC Load Balancing Advisory with service-level goals for each service for which load balancing is enabled.

You can configure the Oracle RAC Load Balancing Advisory for `SERVICE_TIME` or `THROUGHPUT`. Set the connection load-balancing goal to **SHORT**.

You create and modify Oracle Database services using the `srvctl` utility.

To create and modify a 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 => 'wcpedg.example.com',
NETWORK_NAME => 'wcpedg.example.com'
);
```

**Note:**

For the Service Name of the Oracle RAC database, use lowercase letters, followed by the domain name. For example:

`wcpedg.example.com`

**Note:**

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

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

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

```
srvctl add service -d wcpdb -s wcpedg.example.com -r wcpdb1,wcpdb2
```

3. Start the service:

```
srvctl start service -d wcpdb -s wcpedg.example.com
```

**Note:**

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

4. Modify the service so it uses the Load Balancing Advisory and the appropriate service-level goals for run-time connection load balancing.

   More specifically, use the following resources in the Oracle Database 12*c Real Application Clusters Administration and Deployment Guide* to set the SERVICE_TIME and THROUGHPUT service-level goals:

   - "Overview of the Load Balancing Advisory"
   - "Configuring Your Environment to Use the Load Balancing Advisory"

## 9.4 Using SecureFiles for Large Objects (LOBs) in an Oracle Database

Beginning with Oracle Database 11g Release 1, Oracle introduced SecureFiles, a new LOB storage architecture. Oracle recommends using SecureFiles for the Oracle Fusion Middleware schemas, in particular for the Oracle SOA Suite schemas.

For more information, see "Using Oracle SecureFiles LOBs" in the *Oracle Database SecureFiles and Large Objects Developer's Guide*.

In Oracle 12*c* Databases, the default setting for using SecureFiles is `PREFERRED` . This means that the database attempts to create a SecureFiles LOB unless a BasicFiles LOB is explicitly specified for the LOB or the parent LOB (if the LOB is in a partition or sub-partition). The Oracle Fusion Middleware schemas do not explicitly specify BasicFiles, which means that Oracle Fusion Middleware LOBs will default to SecureFiles when installed in an Oracle 12*c* database.

For Oracle 11*g* databases, the `db_securefile` system parameter controls the SecureFiles usage policy. This parameter can be modified dynamically. The following options can be used for using SecureFiles:

- `PERMITTED`: allows SecureFiles to be created (This is the default setting for db_securefile. The default storage method uses BasicFiles)
- `FORCE`: create all (new) LOBs as SecureFiles
- `ALWAYS`: try to create LOBs as SecureFiles, but fall back to BasicFiles if not possible (if ASSM is disabled)

Other values for the `db_securefile` parameter are:

- `IGNORE`: ignore attempts to create SecureFiles
- `NEVER`: disallow new SecureFiles creations

For Oracle 11*g* Databases, Oracle recommends that you set the `db_securefile` parameter to `FORCE` before creating the Oracle Fusion Middleware schemas with the Repository Creation Utility (RCU).

Note that the SecureFiles segments require tablespaces managed with automatic segment space management (ASSM). This means that LOB creation on SecureFiles will fail if ASSM is not enabled. However, the Oracle Fusion Middleware tablespaces are created by default with ASSM enabled. As a result, with the default configuration, nothing needs to be changed to enable SecureFiles for the Oracle Fusion Middleware schemas.

## 9.5 About Database Backup Strategies

This section provides brief information about the necessity of database backup strategies.

At key points in the installation and configuration of an enterprise deployment, this guide recommends that you back up your current environment. For example, after you install the product software and create the schemas for a particular Oracle Fusion Middleware product, you should perform a database backup. Performing a backup allows you to perform a quick recovery from any issue that might occur in the later configuration steps.

You can choose to use your own backup strategy for the database, or you can simply make a backup using operating system tools or RMAN for this purpose.

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

# Part III

# Configuring the Enterprise Deployment

Part III contains the following chapters:

Creating the Initial Infrastructure Domain for an Enterprise Deployment

Configuring the Web Tier for an Enterprise Deployment

Extending the Domain with Oracle WebCenter Portal

Extending the Domain to Include Oracle WebCenter Content

This chapter describes how to extend the enterprise deployment domain with the Oracle WebCenter Content software.

Extending the Domain to Include Inbound Refinery

Extending the Domain with Oracle SOA Suite

Integrating WebCenter Portal Workflows with Oracle SOA Suite in the Same Domain

WebCenter Portal provides several prebuilt workflows that handle portal membership notifications, portal subscription requests, and so on. WebCenter Portal workflows rely on the Oracle BPM Worklist, which is installed as a component of Oracle SOA Suite.

# 10

# Creating the Initial Infrastructure Domain for an Enterprise Deployment

The following topics describe how to install and configure an initial domain, which can be used as the starting point for an enterprise deployment. Later chapters in this guide describe how to extend this initial domain with the various products and components that comprise the enterprise topology you are deploying.

Variables Used When Creating the Infrastructure Domain
: As you perform the tasks in this chapter, you will be referencing the directory variables listed in this section.

Understanding the Initial Infrastructure Domain
: Before you create the initial Infrastructure domain, be sure to review the following key concepts.

Installing the Oracle Fusion Middleware Infrastructure in Preparation for an Enterprise Deployment
: Use the following sections to install the Oracle Fusion Middleware Infrastructure software in preparation for configuring a new domain for an enterprise deployment.

Creating the Database Schemas
: Before you can configure a Fusion Middleware Infrastructure domain, you must install the schemas listed in this section in a certified database for use with this release of Oracle Fusion Middleware.

Configuring the Infrastructure Domain
: The following topics provide instructions for creating a WebLogic Server domain using the Fusion Middleware Configuration wizard.

Configuring the Domain Directories and Starting the Servers on WCPHOST1
: After the domain is created and the node manager is configured, you can then configure the additional domain directories and start the Administration Server and the Managed Servers on WCPHOST1.

Propagating the Domain and Starting the Servers on WCPHOST2
: After you start and validate the Administration Server and WLS_WSM1 Managed Server on WCPHOST1, you can then perform the following tasks on WCPHOST2.

Modifying the Upload and Stage Directories to an Absolute Path
: After configuring the domain and unpacking it to the Managed Server domain directories on all the hosts, verify and update the `upload` and `stage` directories for the new Managed Servers.

Creating a New LDAP Authenticator and Provisioning Enterprise Deployment Users and Group

When you configure an Oracle Fusion Middleware domain, the domain is configured by default to use the WebLogic Server authentication provider (`DefaultAuthenticator`). However, for an enterprise deployment, Oracle recommends that you use a dedicated, centralized LDAP-compliant authentication provider.

Adding the wsm-pm Role to the Administrators Group

After you configure a new LDAP-based Authorization Provider and restart the Administration Server, add the enterprise deployment administration LDAP group (`WCPAdministrators`) as a member to the `policy.Updater` role in the `wsm-pm` application stripe.

Configuring the WebLogic Proxy Plug-In

## 10.1 Variables Used When Creating the Infrastructure Domain

As you perform the tasks in this chapter, you will be referencing the directory variables listed in this section.

These directory variables are defined in File System and Directory Variables Used in This Guide.

- ORACLE_HOME
- ASERVER_HOME
- MSERVER_HOME
- APPLICATION_HOME
- JAVA_HOME
- NM_HOME

In addition, you'll be referencing the following virtual IP (VIP) addresses and host names defined in Physical and Virtual IP Addresses Required by the Enterprise Topology:

- ADMINVHN
- WCPHOST1
- WCPHOST2
- DBHOST1
- DBHOST2
- SCAN Address for the Oracle RAC Database (DB-SCAN.examle.com)

## 10.2 Understanding the Initial Infrastructure Domain

Before you create the initial Infrastructure domain, be sure to review the following key concepts.

About the Infrastructure Distribution

Characteristics of the Domain

### 10.2.1 About the Infrastructure Distribution

You create the initial Infrastructure domain for an enterprise deployment using the Oracle Fusion Middleware Infrastructure distribution. This distribution contains both the Oracle WebLogic Server software and the Oracle JRF software.

The Oracle JRF software consists of Oracle Web Services Manager, Oracle Application Development Framework (Oracle ADF), Oracle Enterprise Manager Fusion Middleware Control, the Repository Creation Utility (RCU), and other libraries and technologies required to support the Oracle Fusion Middleware products.

Later in this guide, you can then extend the domain to support the Oracle Fusion Middleware products required for your enterprise deployment.

For more information, see "Understanding Oracle Fusion Middleware Infrastructure" in *Understanding Oracle Fusion Middleware*.

### 10.2.2 Characteristics of the Domain

The following table lists some of the key characteristics of the domain you are about to create. By reviewing and understanding these characteristics, you can better understand the purpose and context of the procedures used to configure the domain.

Many of these characteristics are described in more detail in Understanding a Typical Enterprise Deployment.

| Characteristic of the Domain | More Information |
|---|---|
| Uses a separate virtual IP (VIP) address for the Administration Server. | Configuration of the Administration Server and Managed Servers Domain Directories |
| Uses separate domain directories for the Administration Server and the Managed Servers in the domain. | Configuration of the Administration Server and Managed Servers Domain Directories |
| Includes a dedicated cluster for Oracle Web Services Manager | Using Oracle Web Services Manager in the Application Tier |
| Uses a per domain Node Manager configuration. | About the Node Manager Configuration in a Typical Enterprise Deployment |
| Requires a separately installed LDAP-based authentication provider. | Understanding OPSS and Requests to the Authentication and Authorization Stores |

## 10.3 Installing the Oracle Fusion Middleware Infrastructure in Preparation for an Enterprise Deployment

Use the following sections to install the Oracle Fusion Middleware Infrastructure software in preparation for configuring a new domain for an enterprise deployment.

Installing a Supported JDK

Starting the Infrastructure Installer on WCPHOST1

Navigating the Infrastructure Installation Screens

Installing Oracle Fusion Middleware Infrastructure on the Other Host Computers

Checking the Directory Structure

After you install the Oracle Fusion Middleware Infrastructure and create the Oracle home, you should see the directory and sub-directories listed in this topic. The contents of your installation vary based on the options you selected during the installation.

## 10.3.1 Installing a Supported JDK

Oracle Fusion Middleware requires that a certified Java Development Kit (JDK) is installed on your system. See the following sections for more information:

Locating and Downloading the JDK Software

Installing the JDK Software

### 10.3.1.1 Locating and Downloading the JDK Software

To find a certified JDK, see the certification document for your release on the Oracle Fusion Middleware Supported System Configurations page.

After you identify the Oracle JDK for the current Oracle Fusion Middleware release, you can download an Oracle JDK from the following location on Oracle Technology Network:

```
http://www.oracle.com/technetwork/java/index.html
```

Be sure to navigate to the download for the Java SE JDK.

### 10.3.1.2 Installing the JDK Software

Install the JDK in the following locations:

- On the shared storage device, where it will be accessible from each of the application tier host computers. Install the JDK in the `/u01/oracle/products/jdk` directory.
- On the local storage device for each of the Web tier host computers.

  The Web tier host computers, which reside in the DMZ, do not necessarily have access to the shared storage on the application tier.

For more information about the recommended location for the JDK software, see the Understanding the Recommended Directory Structure for an Enterprise Deployment.

The following example describes how to install a recent version of JDK 1.8:

1. Change directory to the location where you downloaded the JDK archive file.

2. Unpack the archive into the JDK home directory, and then run these commands:

   ```
   cd download_dir
   tar -xzvf jdk-8u74-linux-x64.tar.gz
   ```

   Note that the JDK version listed here was accurate at the time this document was published. For the latest supported JDK, see the *Oracle Fusion Middleware System Requirements and Specifications* for the current Oracle Fusion Middleware release.

3. Move the JDK directory to the recommended location in the directory structure.

   For example:

```
mv ./jdk1.8.0_74/u01/oracle/products/jdk
```

For more information, see File System and Directory Variables Used in This Guide.

4. Define the *JAVA_HOME* and *PATH* environment variables for running Java on the host computer.

   For example:

   ```
   export JAVA_HOME=/u01/oracle/products/jdk
   export PATH=$JAVA_HOME/bin:$PATH
   ```

5. Run the following command to verify that the appropriate `java` executable is in the path and your environment variables are set correctly:

   ```
   java -version
     java version "1.8.0_74"
     Java(TM) SE Runtime Environment (build 1.8.0_74-b02)
     Java HotSpot(TM) 64-Bit Server VM (build 25.74-b02, mixed mode)
   ```

## 10.3.2 Starting the Infrastructure Installer on WCPHOST1

To start the installation program, perform the following steps.

1. Log in to WCPHOST1.
2. Go to the directory where you downloaded the installation program.
3. Launch the installation program by invoking the `java` executable from the JDK directory on your system, as shown in the example below.

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

   In this example:

   - Replace *JAVA_HOME* with the environment variable or actual JDK location on your system.
   - Replace *distribution_file_name* with the actual name of the distribution JAR file.

     Note that if you download the distribution from the Oracle Technology Network (OTN), then the JAR file is typically packaged inside a downloadable ZIP file.

     To install the software required for the initial Infrastructure domain, the distribution you want to install is **fmw_12.2.1.1.0_infrastructure_generic.jar**.

     For more information about the actual file names of each distribution, see Identifying and Obtaining Software Downloads for an Enterprise Deployment.

When the installation program appears, you are ready to begin the installation. See Navigating the Installation Screens for a description of each installation program screen.

## 10.3.3 Navigating the Infrastructure Installation Screens

The installation program displays a series of screens, in the order listed in the following table.

If you need additional help with any of the installation screens, click the screen name.

| Screen | Description |
|---|---|
| Installation Inventory Setup | On UNIX operating systems, this screen will appear if this is the first time you are installing any Oracle product on this host. Specify the location where you want to create your central inventory. Make sure that the operating system group name selected on this screen has write permissions to the central inventory location.<br>For more information about the central inventory, see Understanding the Oracle Central Inventory in *Installing Software with the Oracle Universal Installer*. |
| Welcome | This screen introduces you to the product installer. |
| Auto Updates | Use this screen to automatically search My Oracle Support for available patches or automatically search a local directory for patches that you've already downloaded for your organization. |
| Installation Location | Use this screen to specify the location of your Oracle home directory.<br>For the purposes of an enterprise deployment, enter the value of the *ORACLE_HOME* variable listed in Table 7-2. |
| Installation Type | Use this screen to select the type of installation and consequently, the products and feature sets you want to install.<br>For this topology, select **Fusion Middleware Infrastructure**.<br>**Note:** The topology in this document does not include server examples. Oracle strongly recommends that you do not install the examples into a production environment. |
| Prerequisite Checks | This screen verifies that your system meets the minimum necessary requirements.<br>If there are any warning or error messages, refer to the Oracle Fusion Middleware System Requirements and Specifications document on the Oracle Technology Network (OTN). |
| Security Updates | If you already have an Oracle Support account, use this screen to indicate how you would like to receive security updates.<br>If you do not have one and are sure you want to skip this step, clear the check box and verify your selection in the follow-up dialog box. |
| Installation Summary | Use this screen to verify the installation options you selected. If you want to save these options to a response file, click **Save Response File** and provide the location and name of the response file. Response files can be used later in a silent installation situation.<br>For more information about silent or command-line installation, see Using the Oracle Universal Installer in Silent Mode in *Installing Software with the Oracle Universal Installer*. |
| Installation Progress | This screen allows you to see the progress of the installation. |
| Installation Complete | This screen appears when the installation is complete. Review the information on this screen, then click **Finish** to dismiss the installer. |

### 10.3.4 Installing Oracle Fusion Middleware Infrastructure on the Other Host Computers

If you have configured a separate shared storage volume or partition for WCPHOST2, then you must also install the Infrastructure on WCPHOST2.

For more information, see Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment.

To install the software on the other host computers in the topology, log in to each host, and use the instructions in Starting the Infrastructure Installer on WCPHOST1 and Navigating the Infrastructure Installation Screens to create the Oracle home on the appropriate storage device.

---

**Note:**

In previous releases, the recommended enterprise topology included a colocated set of Oracle HTTP Server instances. In those releases, there was a requirement to install the Infrastructure on the Web Tier hosts (WEBHOST1 and WEBHOST2). However, for this release, the enterprise deployment topology assumes the Web servers are installed and configured in standalone mode, so they are not considered part of the application tier domain. For more information, see Configuring the Web Tier for an Enterprise Deployment

---

### 10.3.5 Checking the Directory Structure

After you install the Oracle Fusion Middleware Infrastructure and create the Oracle home, you should see the directory and sub-directories listed in this topic. The contents of your installation vary based on the options you selected during the installation.

To check the directory structure:

1. Change to the *ORACLE_HOME* directory where you installed the Infrastructure.
2. Enter the following command:

   ```
   ls --l
   ```

   The directory structure on your system should match the structure shown in the following example:

   ```
   /u01/oracle/products/fmw/

   cfgtoollogs
   coherence
   em
   install
   inventory
   OPatch
   oracle_common
   oraInst.loc
   oui
   root.sh
   wlserver
   ```

For more information about the directory structure after the installation complete, see What are the Key Oracle Fusion Middleware Directories? in *Understanding Oracle Fusion Middleware*.

## 10.4 Creating the Database Schemas

Before you can configure a Fusion Middleware Infrastructure domain, you must install the schemas listed in this section in a certified database for use with this release of Oracle Fusion Middleware.

- Metadata Services (MDS)
- Audit Services (IAU)
- Audit Services Append (IAU_APPEND)
- Audit Services Viewer (IAU_VIEWER)
- Oracle Platform Security Services (OPSS)
- User Messaging Service (UMS)
- WebLogic Services (WLS)
- Common Infrastructure Services (STB)

You use the Repository Creation Utility (RCU) to create the schemas. This utility is installed in the Oracle home for each Oracle Fusion Middleware product. For more information about RCU and how the schemas are created and stored in the database, see "Preparing for Schema Creation" in *Creating Schemas with the Repository Creation Utility*.

Follow the instructions in this section to install the required schemas.

Installing and Configuring a Certified Database

Starting the Repository Creation Utility (RCU)

Navigating the RCU Screens to Create the Schemas

### 10.4.1 Installing and Configuring a Certified Database

Make sure you have installed and configured a certified database, and that the database is up and running.

For more information, see the Preparing the Database for an Enterprise Deployment.

### 10.4.2 Starting the Repository Creation Utility (RCU)

To start the Repository Creation Utility (RCU):

1. Set the *JAVA_HOME* environment variable so it references the location where you installed a supported JDK.

   For more information, see File System and Directory Variables Used in This Guide.

2. Navigate to the following directory on WCPHOST1:

   ```
   ORACLE_HOME/oracle_common/bin
   ```

3. Start RCU:

```
./rcu
```

### 10.4.3 Navigating the RCU Screens to Create the Schemas

Follow the instructions in this section to create the schemas for the Fusion Middleware Infrastructure domain:

- Task 1, "Introducing RCU"
- Task 2, "Selecting a Method of Schema Creation"
- Task 3, "Providing Database Credentials"
- Task 4, "Specifying a Custom Prefix and Selecting Schemas"
- Task 5, "Specifying Schema Passwords"
- Task 6, "Completing Schema Creation"

**Task 1 Introducing RCU**

Review the Welcome screen and verify the version number for RCU. Click **Next** to begin.

**Task 2 Selecting a Method of Schema Creation**

If you have the necessary permission and privileges to perform DBA activities on your database, select **System Load and Product Load** on the Create Repository screen. The procedure in this document assumes that you have the necessary privileges.

If you do not have the necessary permission or privileges to perform DBA activities in the database, you must select **Prepare Scripts for System Load** on this screen. This option will generate a SQL script, which can be provided to your database administrator. See "Understanding System Load and Product Load" in *Creating Schemas with the Repository Creation Utility*.

> **Tip:**
> For more information about the options on this screen, see "Create repository" in *Creating Schemas with the Repository Creation Utility*.

**Task 3 Providing Database Credentials**

On the Database Connection Details screen, provide the database connection details for RCU to connect to your database.

In the **Host Name** field, enter the SCAN address of the Oracle RAC Database.

Click **Next** to proceed, then click **OK** in the dialog window confirming that connection to the database was successful.

> **Tip:**
> For more information about the options on this screen, see "Database Connection Details" in *Creating Schemas with the Repository Creation Utility*.

### Task 4 Specifying a Custom Prefix and Selecting Schemas

1. Specify the custom prefix you want to use to identify the Oracle Fusion Middleware schemas.

   **Note:** Custom prefixes must be 10 characters or less when including WebCenter Portal schemas even though the RCU limit is 12 characters. This is to avoid RCU errors when validating the full WebCenter Portal schemas names. Maximum schema user name length is limited to 30 characters total. WebCenter Portal schema suffixes use up to 20 characters.

   The custom prefix is used to logically group these schemas together for use in this domain. For the purposes of this guide, use the prefix `FMW1221`.

   **Tip:**

   Make a note of the custom prefix you choose to enter here; you will need this later, during the domain creation process.

   For more information about custom prefixes, see "Understanding Custom Prefixes" in *Creating Schemas with the Repository Creation Utility*.

2. Select **AS Common Schemas**.

   When you select **AS Common Schemas**, all of the schemas in this section are automatically selected.

   If the schemas in this section are not automatically selected, then select the required schemas.

A schema called **Common Infrastructure Services** is also automatically created; this schema is grayed out and cannot be selected or deselected. This schema (the STB schema) enables you to retrieve information from RCU during domain configuration. For more information, see "Understanding the Service Table Schema" in *Creating Schemas with the Repository Creation Utility*.

**Tip:**
For more information about how to organize your schemas in a multi-domain environment, see "Planning Your Schema Creation" in *Creating Schemas with the Repository Creation Utility*.

Click **Next** to proceed, then click **OK** on the dialog window confirming that prerequisite checking for schema creation was successful.

### Task 5 Specifying Schema Passwords

Specify how you want to set the schema passwords on your database, then specify and confirm your passwords.

**Tip:**
You must make a note of the passwords you set on this screen; you will need them later on during the domain creation process.

### Task 6 Completing Schema Creation

Navigate through the remainder of the RCU screens to complete schema creation.

For the purposes of this guide, you can accept the default settings on the remaining screens, or you can customize how RCU creates and uses the required tablespaces for the Oracle Fusion Middleware schemas.

For more information about RCU and its features and concepts, see *Creating Schemas with the Repository Creation Utility*.

When you reach the Completion Summary screen, click **Close** to dismiss RCU.

## 10.5 Configuring the Infrastructure Domain

The following topics provide instructions for creating a WebLogic Server domain using the Fusion Middleware Configuration wizard.

For more information on other methods available for domain creation, see Additional Tools for Creating, Extending, and Managing WebLogic Domains in *Creating WebLogic Domains Using the Configuration Wizard*.

Starting the Configuration Wizard

Navigating the Configuration Wizard Screens to Configure the Infrastructure Domain

### 10.5.1 Starting the Configuration Wizard

To begin domain configuration, run the following command in the Oracle Fusion Middleware Oracle home.

```
ORACLE_HOME/oracle_common/common/bin/config.sh
```

### 10.5.2 Navigating the Configuration Wizard Screens to Configure the Infrastructure Domain

Follow the instructions in this section to create and configure the domain for the topology.

**Task 1 Selecting the Domain Type and Domain Home Location**

On the Configuration Type screen, select **Create a new domain**.

In the Domain Location field, specify the value of the *ASERVER_HOME* variable, as defined in File System and Directory Variables Used in This Guide.

> **Tip:**
> More information about the other options on this screen of the Configuration Wizard, see "Configuration Type" in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 2 Selecting the Configuration Templates**

On the Templates screen, make sure **Create Domain Using Product Templates** is selected, then select the following templates:

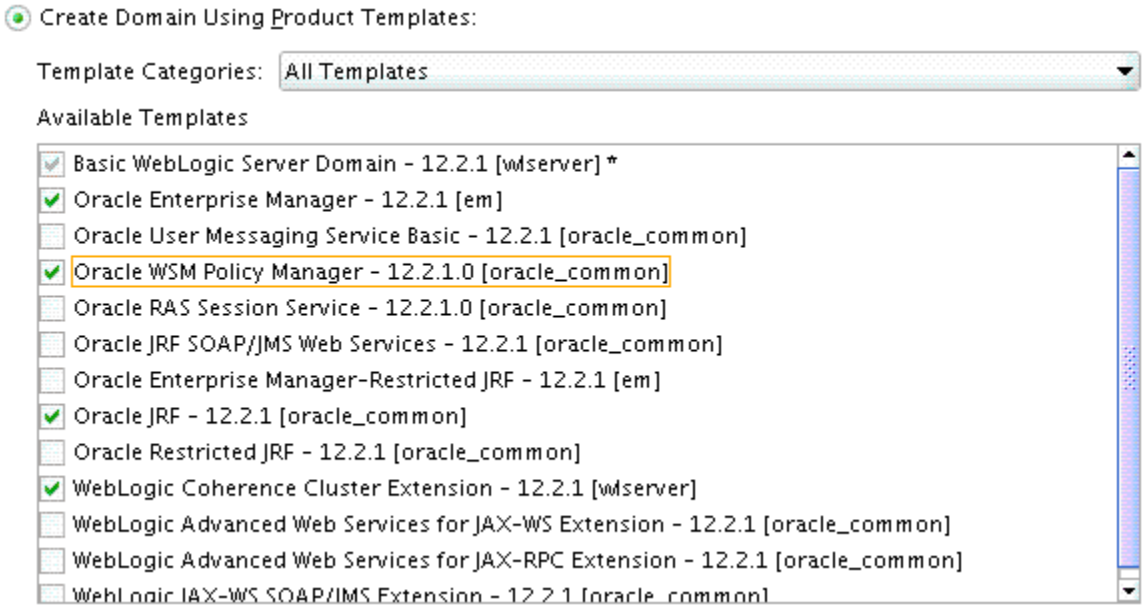
- **Oracle Enterprise Manager - 12.2.1.1.0 [em]**

  Selecting this template automatically selects the following dependencies:

  – Oracle JRF - 12.2.1.1.0 [oracle_common]

  - WebLogic Coherence Cluster Extension - 12.2.1.1 [wlserver]

- **Oracle WSM Policy Manager - 12.2.1.1 [oracle_common]**




**Tip:**
More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 3 Selecting the Application Home Location

On the Application Location screen, specify the value of the *APPLICATION_HOME* variable, as defined in File System and Directory Variables Used in This Guide.

**Tip:**
More information about the options on this screen can be found in Application Location in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 4 Configuring the Administrator Account

On the Administrator Account screen, specify the user name and password for the default WebLogic Administrator account for the domain.

Make a note of the user name and password specified on this screen; you will need these credentials later to boot and connect to the domain's Administration Server.

### Task 5 Specifying the Domain Mode and JDK

On the Domain Mode and JDK screen:

- Select **Production** in the Domain Mode field.
- Select the **Oracle Hotspot** JDK in the JDK field.

Selecting **Production Mode** on this screen gives your environment a higher degree of security, requiring a user name and password to deploy applications and to start the Administration Server.

**Tip:**
More information about the options on this screen, including the differences between development mode and production mode, can be found in Domain Mode and JDK in *Creating WebLogic Domains Using the Configuration Wizard*.

In production mode, a boot identity file can be created to bypass the need to provide a user name and password when starting the Administration Server. For more information, see Creating the boot.properties File.

### Task 6 Specifying the Database Configuration Type

Select **RCU Data** to activate the fields on this screen.

The **RCU Data** option instructs the Configuration Wizard to connect to the database and Service Table (STB) schema to automatically retrieve schema information for the schemas needed to configure the domain.

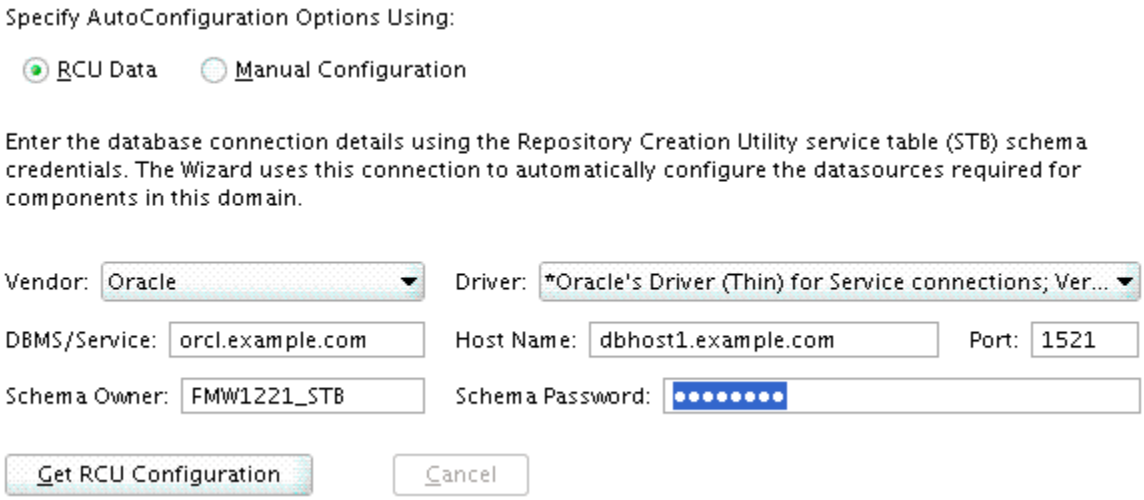
**Note:**
If you choose to select **Manual Configuration** on this screen, you will have to manually fill in the parameters for your schema on the JDBC Component Schema screen.

After selecting **RCU Data**, fill in the fields as shown in the following table. Refer to Figure 10-1 for a partial screen shot of a sample Database Configuration Type screen.

| Field | Description |
|---|---|
| DBMS/Service | Enter the service name for the Oracle RAC database where you will install the product schemas. For example:<br>`orcl.example.com`<br>Be sure this is the common service name that is used to identify all the instances in the Oracle RAC database; do not use the host-specific service name. |
| Host Name | Enter the Single Client Access Name (SCAN) Address for the Oracle RAC database, which you entered in the *Enterprise Deployment Workbook*. |
| Port | Enter the port number on which the database listens. For example, `1521`. |

| Field | Description |
|---|---|
| Schema Owner<br>Schema Password | Enter the user name and password for connecting to the database's Service Table schema.<br>This is the schema user name and password that was specified for the Service Table component on the "Schema Passwords" screen in RCU (see Creating the Database Schemas).<br>The default user name is *prefix*_STB, where *prefix* is the custom prefix that you defined in RCU. |

***Figure 10-1 Setting the Database Configuration Type for an Enterprise Deployment***




Click **Get RCU Configuration** when you are finished specifying the database connection information. The following output in the Connection Result Log indicates that the operating succeeded:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK

Successfully Done.
```

Click **Next** if the connection to the database is successful.

> **Tip:**
> More information about the **RCU Data** option can be found in "Understanding the Service Table Schema" in *Creating Schemas with the Repository Creation Utility*.
>
> More information about the other options on this screen can be found in Datasource Defaults in *Creating WebLogic Domains Using the Configuration Wizard*

### Task 7 Specifying JDBC Component Schema Information

Verify that the values on the JDBC Component Schema screen are correct for all schemas.

The schema table should be populated, because you selected **Get RCU Data** on the previous screen. As a result, the Configuration Wizard locates the database connection values for all the schemas required for this domain.

At this point, the values are configured to connect to a single-instance database. However, for an enterprise deployment, you should use a highly available Real Application Clusters (RAC) database, as described in Preparing the Database for an Enterprise Deployment.

In addition, Oracle recommends that you use an Active GridLink datasource for each of the component schemas. For more information about the advantages of using GridLink data sources to connect to a RAC database, see "Database Considerations" in the *High Availability Guide*.

To convert the data sources to GridLink:

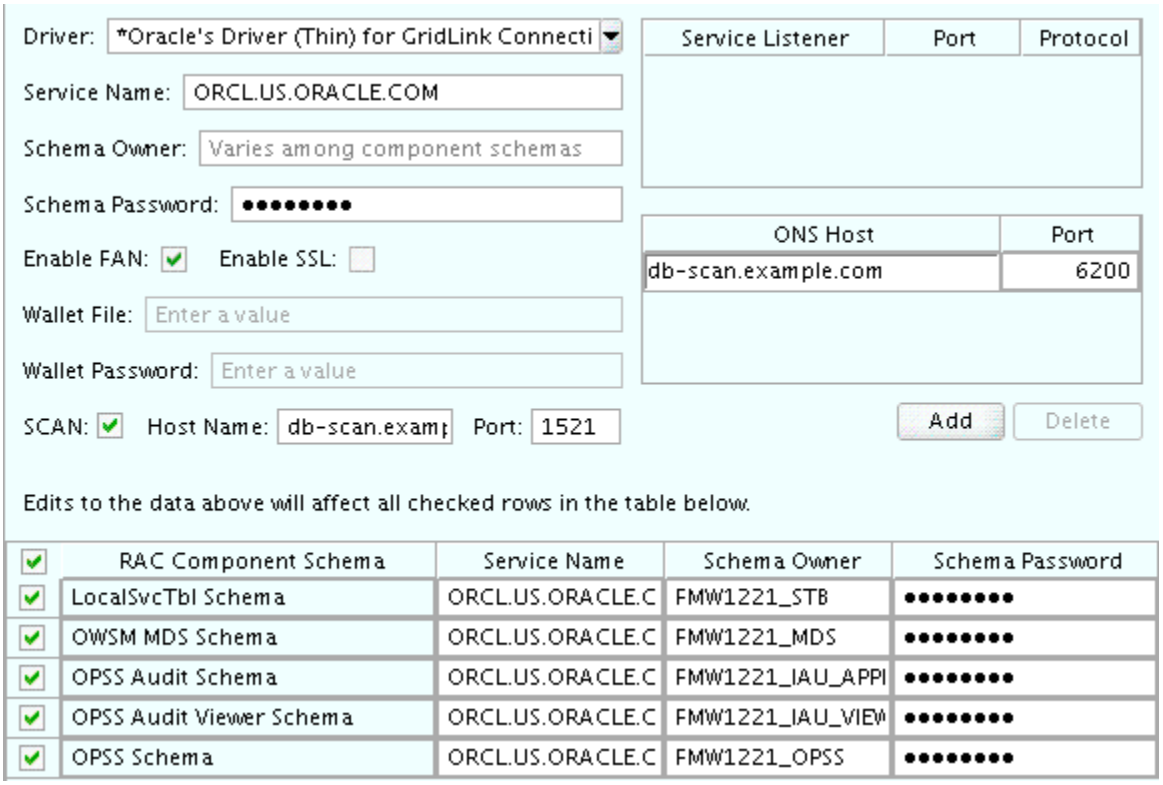
1. Select all the schemas by selecting the checkbox at in the first header row of the schema table.
2. Click **Convert to GridLink** and click **Next**.

### Task 8 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, provide the information required to connect to the RAC database and component schemas, as shown in following table.

| Element | Description and Recommended Value |
|---|---|
| SCAN, Host Name, and Port | Select the **SCAN** check box.<br>In the **Host Name** field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database.<br>In the **Port** field, enter the SCAN listening port for the database (for example, `1521`) |
| ONS Host and Port | In the **ONS Host** field, enter the SCAN address for the Oracle RAC database.<br>In the **Port** field, enter the ONS Remote port (typically, `6200`). |
| Enable Fan | Verify that the **Enable Fan** check box is selected, so the database can receive and process FAN events. |

***Figure 10-2 Sample Values for the GridLink Oracle RAC Component Schema Scree***




For more information about specifying the information on this screen, as well as information about how to identify the correct SCAN address, see "Configuring Active GridLink Data Sources with Oracle RAC" in the *High Availability Guide*.

You can also click **Help** to display a brief description of each field on the screen.

### Task 9 Testing the JDBC Connections

Use the JDBC Component Schema Test screen to test the data source connections you have just configured.

A green check mark in the Status column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

> **Tip:**
> More information about the other options on this screen can be found in Test Component Schema in *Creating WebLogic Domains Using the Configuration Wizard*

### Task 10 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

- **Administration Server**

  This is required to properly configure the listen address of the Administration Server.

- **Node Manager**

  This is required to configure Node Manager.

- **Topology**

  This is required to configure the Managed Servers and cluster, and also for configuring the machine and targeting the Managed Servers to the machine.

- **File Store**

  This is required to configure the appropriate shared storage for JMS persistent stores.

---

**Note:**
When using the Advanced Configuration screen in the Configuration Wizard:

- If any of the above options are not available on the screen, then return to the Templates screen, and be sure you selected the required templates for this topology.
- Do not select the **Domain Frontend Host Capture** advanced configuration option. You will later configure the frontend host property for specific clusters, rather than for the domain.

---

### Task 11 Configuring the Administration Server Listen Address

On the Administration Server screen:

1. In the **Server Name** field, retain the default value - AdminServer.
2. In the **Listen Address** field, enter the virtual host name that corresponds to the VIP of the ADMINVHN that you procured in Procuring Resources for an Enterprise Deployment and enabled in Preparing the Host Computers for an Enterprise Deployment.

   For more information on the reasons for using the ADMINVHN virtual host, see Reserving the Required IP Addresses for an Enterprise Deployment.
3. Leave the other fields at their default values.

   In particular, be sure that no server groups are assigned to the Administration Server.

### Task 12 Configuring Node Manager

Select **Per Domain Default Location** as the Node Manager type, then specify the Node Manager credentials you will use to connect to the Node Manager.

**Tip:**
For more information about the options on this screen, see "Node Manager" in *Creating WebLogic Domains Using the Configuration Wizard*.

For more information about per domain and per host Node Manager implementations, see About the Node Manager Configuration in a Typical Enterprise Deployment.

For additional information, see "Configuring Node Manager on Multiple Machines" in *Administering Node Manager for Oracle WebLogic Server*.

### Task 13 Configuring Managed Servers

Use the Managed Servers screen to create two new Managed Servers:

1. Click the **Add** button to create a new Managed Server.
2. Specify `WLS_WSM1` in the **Server name** column.
3. In the **Listen Address** column, enter *WCPHOST1*.

   Be sure to enter the host name that corresponds to WCPHOST1; do not use the IP address.
4. In the **Listen Port** column, enter `7010`.
5. In the **Server Groups** drop-down list, select **JRF-MAN-SVR**, **WSM-CACHE-SVR**, and **WSMPM-MAN-SVR**. (See Figure 10-3.)

   These server groups ensure that the Oracle JRF and Oracle Web Services Manager (OWSM) services are targeted to the Managed Servers you are creating.

   Server groups target Fusion Middleware applications and services to one or more servers by mapping defined groups of application services to each defined server group. Any application services that are mapped to a given server group are automatically targeted to all servers that are assigned to that group. For more information, see "Application Service Groups, Server Groups, and Application Service Mappings" in *Domain Template Reference*.

   **Note:**

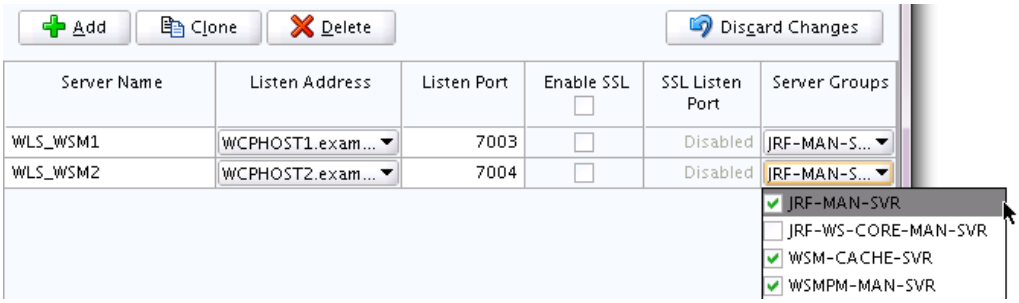
   Nonce caching for Oracle Web Services is configured automatically by the WSM-CACHE-SVR server group and is suitable for most applications. Nonce is a unique number that can be used only once in a SOAP request and is used to prevent replay attacks. Nonce caching will naturally scale with the number of added Managed Servers running Web service applications.

   For advanced caching configurations, see "Caching the Nonce with Oracle Coherence" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*, which provides additional guidance for the use of nonce caching and the WSM-CACHE-SVR server-group.
6. Repeat this process to create a second Managed Server named `WLS_WSM2`.

   For the **Listen Address**, enter *WCPHOST2*. For the **Listen Port**, enter 7010. Apply the same server groups you applied to the first managed server to the WLS_WSM2.

The Managed Server names suggested in this procedure (WLS_WSM1 and WLS_WSM2) will be referenced throughout this document; if you choose different names then be sure to replace them as needed.

***Figure 10-3 Using the Configuration Wizard to Define Managed Servers for an Enterprise Deployment***

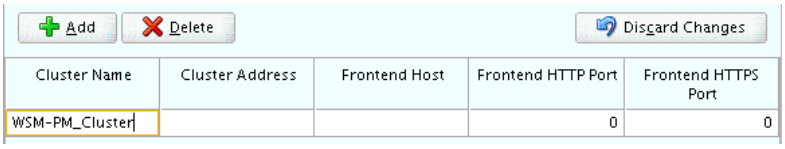



**Tip:**
More information about the options on this screen can be found in Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 14 Configuring a Cluster

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify `WSM-PM_Cluster` in the **Cluster Name** field.
3. Leave the other fields empty.




**Tips:**
For more information about the options on this screen, see "Clusters" in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 15 Assigning Managed Servers to the Cluster

Use the Assign Servers to Clusters screen to assign `WLS_WSM1` and `WLS_WSM2` to the new cluster `WSM-PM_Cluster`:

1. In the **Clusters** pane, select the cluster to which you want to assign the servers; in this case, `WSM-PM_Cluster`.
2. In the **Servers** pane, assign `WLS_WSM1` to `WSM-PM_Cluster` by doing one of the following:
   - Click once on `WLS_WSM1` to select it, then click on the right arrow to move it beneath the selected cluster (`WSM-PM_Cluster`) in the Clusters pane.

OR

- Double-click on `WLS_WSM1` to move it beneath the selected cluster (`WSM-PM_Cluster`) in the clusters pane.

3. Repeat these steps to assign the WLS_WSM2 Managed Server to the WSM-PM_Cluster.


**Tip:**
More information about the options on this screen can be found in Assign Servers to Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 16 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain.

In the **Cluster Listen Port**, enter `9991`.

**Note:**
For Coherence licensing information, refer to "Oracle Coherence" in *Oracle Fusion Middleware Licensing Information*.

### Task 17 Creating Machines

Use the Machines screen to create three new machines in the domain. A machine is required in order for the Node Manager to be able to start and stop the servers.

1. Select the **Unix Machine** tab.
2. Click the **Add** button to create three new Unix machines.

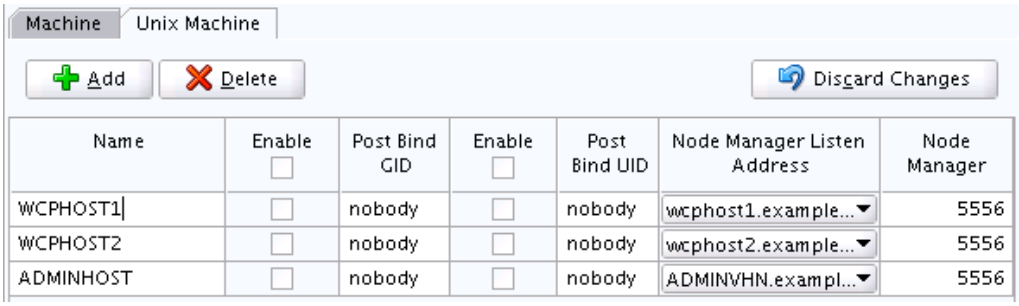
   Use the values in Table 10-1 to define the Name and Node Manager Listen Address of each machine. Figure 10-4 shows a portion of the Machines screen, with example values for each machine.
3. Verify the port in the Node Manager Listen Port field.

   The port number `5556`, shown in this example, may be referenced by other examples in the documentation. Replace this port number with your own port number as needed.

| Name | Node Manager Listen Address | Node Manager Listen Port |
|---|---|---|
| WCPHOST1 | The value of the WCPHOST1 host name variable. For example, `WCPHOST1.example.com`. | 5556 |
| WCPHOST2 | The value of the WCPHOST2 host name variable. For example, `WCPHOST2.example.com`. | 5556 |

| Name | Node Manager Listen Address | Node Manager Listen Port |
|---|---|---|
| ADMINHOST | Enter the value of the ADMINVHN variable. | 5556 |

***Figure 10-4 Example Values for the Configuration Wizard Unix Machines Screen***




**Tip:**
More information about the options on this screen can be found in Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

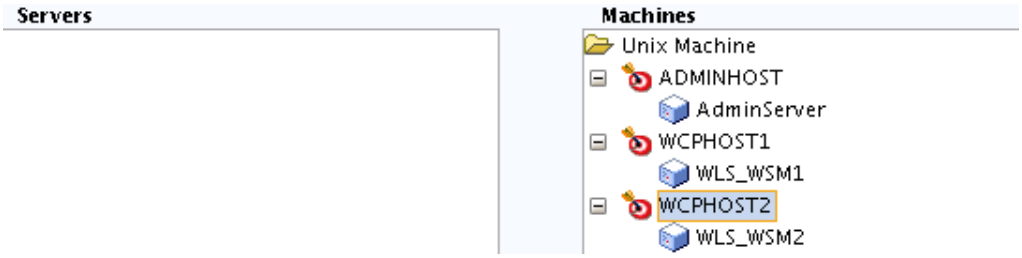
### Task 18 Assigning Servers to Machines

Use the Assign Servers to Machines screen to assign the Administration Server and the two Managed Servers to the appropriate machine.

The Assign Servers to Machines screen is similar to the Assign Managed Servers to Clusters screen. Select the target machine in the Machines column, select the Managed Server in the left column, and click the right arrow to assign the server to the appropriate machine.

Assign the servers as follows:

- Assign the AdminServer to the ADMINHOST machine.
- Assign the WLS-WSM1 Managed Server to the WCPHOST1 machine.
- Assign the WLS-WSM2 Managed Server to the WCPHOST2 machine.




**Tip:**
More information about the options on this screen can be found in Assign Servers to Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 19 Creating Virtual Targets

Click **Next** to proceed to the next screen.

### Task 20 Creating Partitions

Click **Next** to proceed to the next screen.

### Task 21 Configuring the JMS File Store

When you configure a domain using the Oracle WSM Policy Manager configuration template, you should select the proper location of the Metadata Services (MDS) JMS File Store, especially when you are configuring an enterprise deployment.

Enter the following location in the Directory column of the JMS File Store screen:

```
ORACLE_RUNTIME/domain_name/WSM-PM_Cluster/jms
```

> **Note:** You can provide a non-shared storage location for this store. It is used only in WSM's development mode. In the production environments, the database will be used to host it instead.

Replace *ORACLE_RUNTIME* with the actual value of the variable, as defined in File System and Directory Variables Used in This Guide.

Replace *domain_name* with the name of the domain you are creating.

### Task 22 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation will not begin until you click **Create**.

> **Tip:**
> More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 23 Writing Down Your Domain Home and Administration Server URL

The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Administration Server.

Click **Finish** to dismiss the configuration wizard.

## 10.6 Configuring the Domain Directories and Starting the Servers on WCPHOST1

After the domain is created and the node manager is configured, you can then configure the additional domain directories and start the Administration Server and the Managed Servers on WCPHOST1.

Starting the Node Manager in the Administration Server Domain Home on WCPHOST1

Use these steps to start the per-domain Node Manager for the *ASERVER_HOME* domain directory.

Creating the boot.properties File

You must create a `boot.properties` if you want start the Node Manager without being prompted for the Node Manager credentials. This step is required in an enterprise deployment. The credentials you enter in this file are encrypted when you start the Administration Server.

Starting the Administration Server Using the Node Manager

After you have configured the domain and configured the Node Manager, you can start the Administration Server, using the Node Manager. In an enterprise Deployment, the Node Manager is used to start and stop the Administration Server and all the Managed Servers in the domain.

Validating the Administration Server

Before proceeding with the configuration steps, validate that the Administration Server has started successfully by making sure you have access to the Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control, which both are installed and configured on the Administration Servers.

Disabling the Derby Database

Creating a Separate Domain Directory for Managed Servers on WCPHOST1

When you initially create the domain for enterprise deployment, the domain directory resides on a shared disk. This default domain directory will be used to run the Administration Server. You can now create a copy of the domain on the local storage for both WCPHOST1 and WCPHOST2. The domain directory on the local (or private) storage will be used to run the Managed Servers.

Starting the Node Manager in the Managed Server Domain Directory on WCPHOST1

Starting and Validating the WLS_WSM1 Managed Server on WCPHOST1

After you have configured Node Manager and created the Managed Server domain directory, you can use Oracle Enterprise Manager Fusion Middleware Control to start the WLS_WSM1 Managed Server on WCPHOST1.

### 10.6.1 Starting the Node Manager in the Administration Server Domain Home on WCPHOST1

Use these steps to start the per-domain Node Manager for the *ASERVER_HOME* domain directory.

1. Verify that the listen address in the `nodemanager.properties` file is set correctly:
   a. Open the following file, using a text editor:

      *ASERVER_HOME*/nodemanager/nodemanager.properties

   b. Make sure the `ListenAddress` property is set to the value of the ADMINVHN virtual IP address.
2. Navigate to the following directory:

   *ASERVER_HOME*/bin
3. Use the following command to start the Node Manager:

   ```
   nohup ./startNodeManager.sh > ASERVER_HOME/nodemanager/nodemanager.out 2>&1 &
   ```

   For more information about additional Node Manager configuration options, see *Administering Node Manager for Oracle WebLogic Server*.

## 10.6.2 Creating the boot.properties File

You must create a `boot.properties` if you want start the Node Manager without being prompted for the Node Manager credentials. This step is required in an enterprise deployment. The credentials you enter in this file are encrypted when you start the Administration Server.

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

1. Create the following directory structure:

   ```
   mkdir -p ASERVER_HOME/servers/AdminServer/security
   ```
2. In a text editor, create a file called `boot.properties` in the `security` directory created in the previous step, and enter the Administration Server credentials that you defined when you ran the Configuration Wizard to create the domain:

   ```
   username=adminuser
   password=password
   ```

   **Note:**

   When you start the Administration Server, the `username` and `password` entries in the file get encrypted.

   For security reasons, minimize the amount of 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.

## 10.6.3 Starting the Administration Server Using the Node Manager

After you have configured the domain and configured the Node Manager, you can start the Administration Server, using the Node Manager. In an enterprise Deployment, the Node Manager is used to start and stop the Administration Server and all the Managed Servers in the domain.

To start the Administration Server using the Node Manager:

1. Start the WebLogic Scripting Tool (WLST):

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

2. Connect to Node Manager using the Node Manager credentials:

```
wls:/offline>nmConnect('nodemanager_username','nodemanager_password',
            'ADMINVHN','5556','domain_name',
            'ASERVER_HOME')
```

---

**Note:**

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

```
ASERVER_HOME/config/nodemanager
```

---

3. Start the Administration Server:

```
nmStart('AdminServer')
```

---

**Note:**

When you start the Administration Server, it attempts to connect to Oracle Web Services Manager for WebServices policies. It is expected that, since the WSM-PM Managed Servers are not yet started, the following message will appear in the Administration Server log:

```
<Warning><oracle.wsm.resources.policymanager>
<WSM-02141><Unable to connect to the policy access service due to Oracle WSM
policy manager host server being down.>
```

---

4. Exit WLST:

```
exit()
```

## 10.6.4 Validating the Administration Server

Before proceeding with the configuration steps, validate that the Administration Server has started successfully by making sure you have access to the Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control, which both are installed and configured on the Administration Servers.

To navigate to Fusion Middleware Control, enter the following URL, and log in with the Oracle WebLogic Server administrator credentials:

```
ADMINVHN:7001/em
```

To navigate to the Oracle WebLogic Server Administration Console, enter the following URL, and log in with the same administration credentials:

```
ADMINVHN:7001/console
```

### 10.6.5 Disabling the Derby Database

Before you create the Managed Server directory and start the Managed Servers, disable the embedded Derby database, which is a file-based database, packaged with Oracle WebLogic Server. The Derby database is used primarily for development environments. As a result, you must disable it when you are configuring a production-ready enterprise deployment environment; otherwise, the Derby database process will start automatically when you start the Managed Servers.

To disable the Derby database:

1. Navigate to the following directory in the Oracle home.

   *WL_HOME*/common/derby/lib

2. Rename the Derber library jar file:

   ```
   mv derby.jar disable_derby.jar
   ```

3. Complete steps 1 through 2 on each ORACLE_HOME for WCPHOST1 and WCPHOST2 if they use separate shared filesystems.

### 10.6.6 Creating a Separate Domain Directory for Managed Servers on WCPHOST1

When you initially create the domain for enterprise deployment, the domain directory resides on a shared disk. This default domain directory will be used to run the Administration Server. You can now create a copy of the domain on the local storage for both WCPHOST1 and WCPHOST2. The domain directory on the local (or private) storage will be used to run the Managed Servers.

Placing the MSERVER_HOME on local storage is recommended to eliminate the potential contention and overhead cause by servers writing logs to shared storage. It is also faster to load classes and jars need from the domain directory, so any tmp or cache data that Managed Servers use from the domain directory is processed quicker.

As described in Preparing the File System for an Enterprise Deployment, the path to the Administration Server domain home is represented by the ASERVER_HOME variable, and the path to the Managed Server domain home is represented by the MSERVER_HOME variable.

To create the Managed Server domain directory:

1. Log in to WCPHOST1 and run the pack command to create a template as follows:

   ```
   cd ORACLE_COMMON_HOME/common/bin

   ./pack.sh -managed=true
             -domain=ASERVER_HOME
             -template=/full_path/wcpdomaintemplate.jar
             -template_name=wcp_domain_template
   ```

   In this example:

   - Replace *ASERVER_HOME* with the actual path to the domain directory you created on the shared storage device.

- Replace *full_path* with the complete path to the location where you want to create the domain template jar file. You will need to reference this location when you copy or unpack the domain template jar file.
- `wcpdomaintemplate.jar` is a sample name for the jar file you are creating, which will contain the domain configuration files.
- `wcp_domain_template` is the label assigned to the template data stored in the template file.

2. Make a note of the location of the `wcpdomaintemplate.jar` file you just created with the pack command.

   You must specify a full path for the template jar file as part of the `-template` argument to the pack command:

   ```
   SHARED_CONFIG_DIR/domains/template_filename.jar
   ```

   **Tip:**

   For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

3. If you haven't already, create the recommended directory structure for the Managed Server domain on the WCPHOST1 local storage device.

   Use the examples in File System and Directory Variables Used in This Guide as a guide.

4. Run the `unpack` command to unpack the template in the domain directory onto the local storage, as follows:

   ```
   cd ORACLE_COMMON_HOME/common/bin

   ./unpack.sh -domain=MSERVER_HOME \
               -overwrite_domain=true \
               -template=/full_path/wcpdomaintemplate.jar
               -log_priority=DEBUG \
               -log=/tmp/unpack.log \
               -app_dir=APPLICATION_HOME \
   ```

   **Note:**

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

   Additionally, to customize server startup parameters that apply to all servers in a domain, you can create a file called setUserOverrides.sh and configure it to, for example, add custom libraries to the WebLogic Server classpath, specify additional java command line options for running the servers, or specify additional environment variables. Any customizations you add to this file are preserved during domain upgrade operations, and are carried over to remote servers when using the pack and unpack commands.

In this example:

- Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
- Replace *full_path* with the complete path to the location where you created or copied the template jar file.
- `wcpdomaintemplate.jar` is the name of the template jar file you created when you ran the pack command to pack up the domain on the shared storage device.

**Tip:**

For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

5. Change directory to the newly created Managed Server directory and verify that the domain configuration files were copied to the correct location on the WCPHOST1 local storage device.

## 10.6.7 Starting the Node Manager in the Managed Server Domain Directory on WCPHOST1

After you create the Managed Server domain directory, there are two domain home directories and two corresponding Node Manager instances on WCPHOST1. You use one Node Manager to control the Administration Server, running from Administration Server domain home, and you use the other Node Manager to control the Managed Servers, running from the Managed Server domain home.

You must start the two Node Managers independently.

**Note:** The Node Manager for the Managed Server's *MSERVER_HOME* will be reset every time the domain configuration is unpacked. The `ListenAddress` will be changed to the *ADMINVHN* instead of the correct hostname. This needs to be changed to the correct value before starting the Node Manager service after an unpack is performed.

Follow these steps to update and start the Node Manager from the Managed Server home:

1. Verify that the listen address in the `nodemanager.properties` file is set correctly, by completing the following steps:
   a. By using a text editor, open the `nodemanager.properties` file from the `MSERVER_HOME/nodemanager/` directory.
   b. Update the `ListenAddress` property to the correct hostname as follows:
      - `WCPHOST1: ListenAddress=WCPHOST1`
      - `WCPHOST2: ListenAddress=WCPHOST2`
   c. Update the `ListenPort` property with the correct Listen Port details.

2. Navigate to the following directory:

   *MSERVER_HOME*/bin

3. Use the following command to start the Node Manager:

   ```
   nohup ./startNodeManager.sh > $MSERVER_HOME/nodemanager/nodemanager.out 2>&1 &
   ```

For information about additional Node Manager configuration options, see *Administering Node Manager for Oracle WebLogic Server*.

### 10.6.8 Starting and Validating the WLS_WSM1 Managed Server on WCPHOST1

After you have configured Node Manager and created the Managed Server domain directory, you can use Oracle Enterprise Manager Fusion Middleware Control to start the WLS_WSM1 Managed Server on WCPHOST1.

1. Enter the following URL into a browser to display the Fusion Middleware Control login screen:

   http://*ADMINVHN*:7001/em

   In this example:

   - Replace *ADMINVHN* with the host name assigned to the ADMINVHN Virtual IP address in Identifying and Obtaining Software Downloads for an Enterprise Deployment.
   - Port 7001 is the typical port used for the Administration Server console and Fusion Middleware Control. However, you should use the actual URL that was displayed at the end of the Configuration Wizard session when you created the domain.

     **Tip:**

     For more information about managing Oracle Fusion Middleware using Oracle Enterprise Manager Fusion Middleware, see "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control" in *Administering Oracle Fusion Middleware*.

2. Log in to Fusion Middleware Control using the Administration Server credentials.
3. Select the **Servers** pane to view the Managed Servers in the domain.
4. Select only the **WLS_WSM1** Managed Server, and then click **Control** > **Start** on the tool bar.
5. To verify that the Managed Server is working correctly, open your browser and enter the following URL:

   *WCPHOST1*:7010/wsm-pm/

   Enter the domain admin user name and password when prompted.

## 10.7 Propagating the Domain and Starting the Servers on WCPHOST2

After you start and validate the Administration Server and WLS_WSM1 Managed Server on WCPHOST1, you can then perform the following tasks on WCPHOST2.

## 10.7.1 Unpacking the Domain Configuration on WCPHOST2

Now that you have the Administration Server and the first WLS_WSM1 Managed Server running on WCPHOST1, you can configure the domain on WCPHOST2.

1. Log in to WCPHOST2.

2. If you haven't already, create the recommended directory structure for the Managed Server domain on the WCPHOST2 storage device.

   Use the examples in File System and Directory Variables Used in This Guide as a guide.

3. Make sure the `wcedgdomaintemplate.jar` accessible to WCPHOST2.

   For example, if you are using a separate shared storage volume or partition for WCPHOST2, then copy the template to the volume or partition mounted to WCPHOST2.

4. Run the `unpack` command to unpack the template in the domain directory onto the local storage, as follows:

   ```
   cd ORACLE_COMMON_HOME/common/bin

   ./unpack.sh -domain=MSERVER_HOME
               -overwrite_domain=true
               -template=/full_path/wcedgdomaintemplate.jar
               -log_priority=DEBUG
               -log=/tmp/unpack.log
               -app_dir=APPLICATION_HOME
   ```

   In this example:

   - Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
   - Replace *full_path* with the complete path and file name of the domain template jar file that you created when you ran the pack command to pack up the domain on the shared storage device.
   - Replace *APPLICATION_HOME* with the complete path to the Application directory for the domain on shared storage. For more information, see File System and Directory Variables Used in This Guide.

     **Tip:**

     For more information about the pack and unpack commands, see Overview of the Pack and Unpack Commands in *Creating Templates and Domains Using the Pack and Unpack Commands*.

5. Change directory to the newly created MSERVER_HOME directory and verify that the domain configuration files were copied to the correct location on the WCPHOST2 local storage device.

### 10.7.2 Starting the Node Manager on WCPHOST2

After you have propagated the domain configuration to WCPHOST2, you can update and start the Node Manager for the *MSERVER_HOME* domain directory.

> **Note:** The Node Manager for the Managed Server's *MSERVER_HOME* will be reset every time the domain configuration is unpacked. The `ListenAddress` will be changed to the *ADMINVHN* instead of the correct hostname. This needs to be changed to the correct value before starting the Node Manager service after an unpack is performed.

Follow these steps to update and start the Node Manager from the Managed Server home:

1. Verify that the listen address in the `nodemanager.properties` file is set correctly, by completing the following steps:
   a. By using a text editor, open the `nodemanager.properties` file from the `MSERVER_HOME/nodemanager/` directory.
   b. Update the `ListenAddress` property to the correct `hostname` as follows:
      - WCPHOST1: `ListenAddress=WCPHOST1`
      - WCPHOST2: `ListenAddress=WCPHOST2`
2. Navigate to the following directory:

   ```
   MSERVER_HOME/bin
   ```

3. Use the following command to start the Node Manager:

   ```
   nohup ./startNodeManager.sh > $MSERVER_HOME/nodemanager/nodemanager.out 2>&1 &
   ```

For information about additional Node Manager configuration options, see *Administering Node Manager for Oracle WebLogic Server*.

### 10.7.3 Starting and Validating the WLS_WSM2 Managed Server on WCPHOST2

Use the procedure in Starting and Validating the WLS_WSM1 Managed Server on WCPHOST1 to start and validate the WLS_WSM2 Managed Server on WCPHOST2.

## 10.8 Modifying the Upload and Stage Directories to an Absolute Path

After configuring the domain and unpacking it to the Managed Server domain directories on all the hosts, verify and update the `upload` and `stage` directories for the new Managed Servers.

This step is necessary to avoid potential issues when performing remote deployments and for deployments that require the stage mode.

To update these directory paths for all the Managed Servers in the Managed Server domain home directory:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the left navigation tree, expand **Domain**, and then **Environment**.
3. Click **Lock & Edit**.
4. Click **Servers**.
5. For each new Managed Server in the Managed Server domain home directory:
   a. Click the name of the Managed Server.
   b. Click the **Configuration** tab, and then click the **Deployment** tab.
   c. Verify that the **Staging Directory Name** is set to the following:

      ```
      MSERVER_HOME/servers/server_name/stage
      ```

      Replace *MSERVER_HOME* with the directory path for the MSERVER_HOME directory; replace *server_name* with the name of the Server you are editing.
   d. Update the **Upload Directory Name** to the following value:

      ```
      ASERVER_HOME/servers/AdminServer/upload
      ```

      Replace *ASERVER_HOME* with the directory path for the ASERVER_HOME directory.
   e. Click **Save**.
   f. Return to the Summary of Servers screen.
6. When you have modified these values for each Managed Server, click **Activate Changes**.

## 10.9 Creating a New LDAP Authenticator and Provisioning Enterprise Deployment Users and Group

When you configure an Oracle Fusion Middleware domain, the domain is configured by default to use the WebLogic Server authentication provider (`DefaultAuthenticator`). However, for an enterprise deployment, Oracle recommends that you use a dedicated, centralized LDAP-compliant authentication provider.

The following topics describe how to use the Oracle WebLogic Server Administration Console to create a new authentication provider for the enterprise deployment domain. This procedure assumes you have already installed and configured a supported LDAP directory, such as Oracle Unified Directory or Oracle Internet Directory.

About the Supported Authentication Providers

About the Enterprise Deployment Users and Groups

Prerequisites for Creating a New Authentication Provider and Provisioning Users and Groups

Provisioning a Domain Connector User in the LDAP Directory

Creating the New Authentication Provider

## 10.9.1 About the Supported Authentication Providers

Oracle Fusion Middleware supports a variety of LDAP authentication providers. For more information, see "Identity Store Types and WebLogic Authenticators" in *Securing Applications with Oracle Platform Security Services*.

The instructions in this guide assume you will be using one of the following providers:

- Oracle Unified Directory
- Oracle Internet Directory
- Oracle Virtual Directory

---

**Note:**

By default, the instructions here describe how to configure the identity service instance to support querying against a single LDAP identity store.

However, you can configure the service to support a virtualized identity store, which queries multiple LDAP identity stores, using LibOVD.

For more information about configuring a Multi-LDAP lookup, refer to "Configuring the Identity Store Service" in *Securing Applications with Oracle Platform Security Services*.

---

## 10.9.2 About the Enterprise Deployment Users and Groups

The following topics provide important information on the purpose and characteristics of the enterprise deployment administration users and groups.



### 10.9.2.1 About Using Unique Administration Users for Each Domain

When you use a central LDAP user store, you can provision users and groups for use with multiple Oracle WebLogic Server domains. As a result, there is a possibility that one WebLogic administration user can have access to all the domains within an enterprise.

Such an approach is not recommended. Instead, it is a best practice to assign a unique distinguished name (DN) within the directory tree for the users and groups you provision for the administration of your Oracle Fusion Middleware domains.

For example, if you plan to install and configure an Oracle WebCenter Portal enterprise deployment domain, then create a user called **`weblogic_wcp`** and an administration group called **`WCPAdministrators`**.

#### 10.9.2.2 About the Domain Connector User

Oracle recommends that you create a separate domain connector user (for example, `wcpLDAP`) in your LDAP directory. This user allows the domain to connect to the LDAP directory for the purposes of user authentication. It is recommended that this user be a non-administrative user.

In a typical Oracle Identity and Access Management deployment, you create this user in the `systemids` container. This container is used for system users that are not normally visible to users. Placing the user into the `systemids` container ensures that customers who have Oracle Identity Manager do not reconcile this user.

#### 10.9.2.3 About Adding Users to the Central LDAP Directory

After you configure a central LDAP directory to be the authenticator for the enterprise domain, then you should add all new users to the new authenticator and not to the default WebLogic Server authenticator.

To add new users to the central LDAP directory, you cannot use the WebLogic Administration Console. Instead, you must use the appropriate LDAP modification tools, such as ldapbrowser or JXplorer.

When you are using multiple authenticators (a requirement for an enterprise deployment), login and authentication will work, but role retrieval will not. The role is retrieved from the first authenticator only. If you want to retrieve roles using any other authenticator, then you must enable virtualization for the domain.

Enabling virtualization involves the following steps:

1. Locate and open the following configuration file with a text editor:

   *`DOMAIN_HOME`*`/config/fmwconfig/jps-config.xml`

2. In the *serviceInstance* tag with `name="idstore.ldap"` and `provider="idstore.ldap.provider"`, add or update the following property as follows:

   ```
   <property name="virtualize" value="true"/>
   ```

   For more information about the virtualize property, see "OPSS System and Configuration Properties" in *Securing Applications with Oracle Platform Security Services*.

#### 10.9.2.4 About Product-Specific Roles and Groups for Oracle WebCenter Portal

Each Oracle Fusion Middleware product implements its own predefined roles and groups for administration and monitoring.

As a result, as you extend the domain to add additional products, you can add these product-specific roles to the `WCPAdministrators` group. After they are added to the `WCPAdministrators` group, each product administrator user can administer the domain with the same set of privileges for performing administration tasks.

Instructions for adding additional roles to the `WCPAdministrators` group are provided in Common Configuration and Management Tasks for an Enterprise Deployment.

#### 10.9.2.5 Example Users and Roles Used in This Guide

In this guide, the examples assume that you provision the following administration user and group with the DNs shown below:

- Admin User DN:

  `cn=weblogic_wcp,cn=users,dc=example,dc=com`

- Admin Group DN:

  `cn=WCPAdministrators,cn=groups,dc=example,dc=com`

- Product-specific LDAP Connector User:

  `cn=wcpLDAP,cn=systemids,dc=example,dc=com`

  This is the user you will use to connect WebLogic Managed Servers to the LDAP authentication provider. This user must have permissions to read and write to the Directory Trees:

  ```
  cn=users,dc=example,dc=com
  cn=groups,dc=example,dc=com
  ```

  **Note:**

  When using Oracle Unified Directory, this user will need to be granted membership in the following groups to provide read and write access:

  ```
  cn=orclFAUserReadPrivilegeGroup,cn=groups,dc=example,dc=com
  cn=orclFAUserWritePrivilegeGroup,cn=groups,dc=example,dc=com
  cn=orclFAGroupReadPrivilegeGroup,cn=groups,dc=example,dc=com
  cn=orclFAGroupWritePrivilegeGroup,cn=groups,dc=example,dc=com
  ```

### 10.9.3 Prerequisites for Creating a New Authentication Provider and Provisioning Users and Groups

Before you create a new LDAP authentication provider, 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
```

In addition, back up the `boot.properties` file for the Administration Server in the following directory:

```
DOMAIN_HOME/servers/AdminServer/security
```

### 10.9.4 Provisioning a Domain Connector User in the LDAP Directory

This example shows how to create a user called `wcpLDAP` in the central LDAP directory.

To provision the user in the LDAP provider:

1. Create an ldif file named `domain_user.ldif` with the contents shown below and then save the file:

```
dn: cn=wcpLDAP,cn=systemids,dc=example,dc=com
changetype: add
orclsamaccountname: wcpLDAP
userpassword: password
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: orcluser
objectclass: orcluserV2
mail: wcpLDAP@example.com
givenname: wcpLDAP
sn: wcpLDAP
cn: wcpLDAP
uid: wcpLDAP
```

**Note:**

If you are using Oracle Unified Directory, then add the following four group memberships to the end of the LDIF file to grant the appropriate read/write privileges:

```
dn:
cn=orclFAUserReadPrivilegeGroup,cn=groups,dc=example,dc=com
changetype: modify
add: uniquemember
uniquemember: cn=wcpLDAP,cn=systemids,dc=example,dc=com

dn: cn=orclFAGroupReadPrivilegeGroup,cn=groups,dc=example,dc=com
changetype: modify
add: uniquemember
uniquemember: cn=wcpLDAP,cn=systemids,dc=example,dc=com

dn: cn=orclFAUserWritePrivilegeGroup,cn=groups,dc=example,dc=com
changetype: modify
add: uniquemember
uniquemember: cn=wcpLDAP,cn=systemids,dc=example,dc=com

dn: cn=orclFAGroupWritePrivilegeGroup,cn=groups,dc=example,dc=com
changetype: modify
add: uniquemember
uniquemember: cn=wcpLDAP,cn=systemids,dc=example,dc=com
```

2. Provision the user in the LDAP directory.

   For example, for an Oracle Unified Directory LDAP provider:

```
OUD_INSTANCE_HOME/bin/ldapmodify -a \
                                 -h oudhost.example.com
                                 -D "cn=oudadmin" \
                                 -w password \
                                 -p 1389 \
                                 -f domain_user.ldif
```

   For Oracle Internet Directory:

```
OID_ORACLE_HOME/bin/ldapadd -h oidhost.example.com \
                            -p 3060 \
                            -D cn="orcladmin" \
```

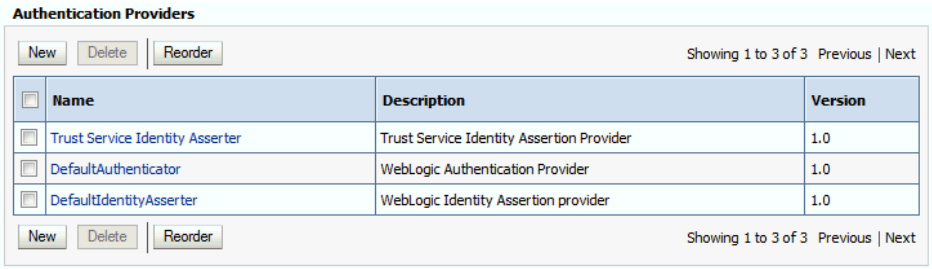
```
-w password \
-c \
-v \
-f domain_user.ldif
```

## 10.9.5 Creating the New Authentication Provider

To configure a new LDAP-based authentication provider:

1. Log in to the WebLogic Server Administration Console.
2. Click **Security Realms** in the left navigational bar.
3. Click the **myrealm** default realm entry.
4. Click the **Providers** tab.

   Note that there is a `DefaultAuthenticator` provider configured for the realm. This is the default WebLogic Server authentication provider.




5. Click **Lock & Edit** in the Change Center.
6. Click the **New** button below the **Authentication Providers** table.
7. Enter a name for the provider.

   Use one of the following names, based on the LDAP directory service you are planning to use as your credential store:

   - `OUDAuthenticator` for Oracle Unified Directory
   - `OIDAuthenticator` for Oracle Internet Directory
   - `OVDAuthenticator` for Oracle Virtual Directory

8. Select the authenticator type from the **Type** drop-down list.

   Select one of the following types, based on the LDAP directory service you are planning to use as your credential store:

   - `OracleUnifiedDirectoryAuthenticator` for Oracle Unified Directory
   - `OracleInternetDirectoryAuthenticator` for Oracle Internet Directory
   - `OracleVirtualDirectoryAuthenticator` for Oracle Virtual Directory

9. Click **OK** to return to the Providers screen.
10. On the Providers screen, click the newly created authenticator in the table.
11. Select **SUFFICIENT** from the **Control Flag** drop-down menu.


Setting the control flag to **SUFFICIENT** indicates that if the authenticator can successfully authenticate a user, then the authenticator 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 flags set to **SUFFICIENT**; in particular, check the **`DefaultAuthenticator`** and make sure that its control flag is set to **SUFFICIENT**.

12. Click **Save** to save the control flag settings.

13. Click the **Provider Specific** tab and enter the details specific to your LDAP server, as shown in the following table.

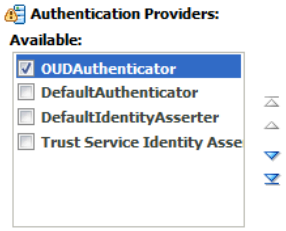
    Note that only the required fields are discussed in this procedure. For information about all the fields on this page, consider the following resources:

    - To display a description of each field, click **Help** on the **Provider Specific** tab.
    - For more information on setting the **User Base DN**, **User From Name Filter**, and **User Attribute** fields, see "Configuring Users and Groups in the Oracle Internet Directory and Oracle Virtual Directory Authentication Providers" in *Administering Security for Oracle WebLogic Server*.

| Parameter | Sample Value | Value Description |
|---|---|---|
| Host | For example: `oud.example.com` | The LDAP server's server ID. |
| Port | For example: `1689` | The LDAP server's port number. |
| Principal | For example: `cn=wcpLDAP, cn=systemids,dc=example,dc=com` | The LDAP user DN used to connect to the LDAP server. |
| Credential | Enter LDAP password. | The password used to connect to the LDAP server. |
| SSL Enabled | Unchecked (clear) | Specifies whether SSL protocol is used when connecting to the LDAP server. |
| User Base DN | For example: `cn=users,dc=example,dc=com` | Specify the DN under which your users start. |

| Parameter | Sample Value | Value Description |
|---|---|---|
| All Users Filter | `(&(uid=*)(objectclass=person))` | Instead of a default search criteria for **All Users Filter**, search all users based on the `uid` value.<br>If the **User Name Attribute** for the user object class in the LDAP directory structure is a type other than `uid`, then change that type in the **User From Name Filter** field.<br>For example, if the **User Name Attribute** type is `cn`, then this field should be set to:<br>`(&(cn=*)(objectclass=person)))` |
| User From Name Filter | For example:<br>`(&(uid=%u)(objectclass=person))` | If the **User Name Attribute** for the user object class in the LDAP directory structure is a type other than `uid`, then change that type in the settings for the **User From Name** Filter.<br>For example, if the **User Name Attribute** type is `cn`, then this field should be set to:<br>`(&(cn=%u)(objectclass=person))).` |
| User Name Attribute | For example: `uid` | The attribute of an LDAP user object that specifies the name of the user. |
| Group Base DN | For example:<br>`cn=groups,dc=example,dc=com` | Specify the DN that points to your Groups node. |
| Use Retrieved User Name as Principal | Checked | Must be turned on. |
| GUID Attribute | `entryuuid` | This value is prepopulated with `entryuuid` when `OracleUnifiedDirectoryAuthenticator` is used for OUD. Check this value if you are using Oracle Unified Directory as your authentication provider. |

14. Click **Save** to save the changes.
15. Return to the Providers page by clicking **Security Realms** in the right navigation pane, clicking the default realm name (**myrealm**), and then **Providers**.
16. Click **Reorder**, and then use the resulting page to make the Provider you just created first in the list of authentication providers.




17. Click **OK**.

18. In the Change Center, click **Activate Changes** .

19. Restart the Administration Server and all managed servers.

    To stop the Managed Servers, log in to Fusion Middleware Control, select the Managed Servers in the Target Navigator and click **Shut Down** in the toolbar.

    To stop and start the Administration Server using the Node Manager:

    a. Start WLST:

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

    b. Connect to Node Manager using the Node Manager credentials you defined in when you created the domain in the Configuration Wizard:

    ```
    wls:/offline>nmConnect('nodemanager_username','nodemanager_password',
                'ADMINVHN','5556','domain_name',
                'ASERVER_HOME')
    ```

    c. Stop the Administration Server:

    ```
    nmKill('AdminServer')
    ```

    d. Start the Administration Server:

    ```
    nmStart('AdminServer')
    ```

    e. Exit WLST:

    ```
    exit()
    ```

    To start the Managed Servers, log in to Fusion Middleware Control, select the Managed Servers, and click **Start Up** in the toolbar.

20. After the restart, review the contents of the following log file:

    ```
    ASERVER_HOME/servers/AdminServer/logs/AdminServer.log
    ```

    Verify that no LDAP connection errors occurred. For example, look for errors such as the following:

    ```
    The LDAP authentication provider named "OUDAuthenticator" failed to make
    connection to ldap server at ...
    ```

    If you see such errors in the log file, then check the authorization provider connection details to verify they are correct and try saving and restarting the Administration Server again.

21. After you restart and verify that no LDAP connection errors are in the log file, try browsing the users and groups that exist in the LDAP provider:

In the Administration Console, navigate to the **Security Realms > myrealm > Users and Groups** page. You should be able to see all users and groups that exist in the LDAP provider structure.

## 10.9.6 Provisioning an Enterprise Deployment Administration User and Group

This example shows how to create a user called **`weblogic_wcp`** and a group called **`WCPAdministrators`**.

To provision the administration user and group in LDAP provider:

1. Create an ldif file named `admin_user.ldif` with the contents shown below and then save the file:

```
dn: cn=weblogic_wcp,cn=users,dc=example,dc=com
changetype: add
orclsamaccountname: weblogic_wcp
userpassword: password
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetorgperson
objectclass: orcluser
objectclass: orcluserV2
mail: weblogic_wcp@example.com
givenname: weblogic_wcp
sn: weblogic_wcp
cn: weblogic_wcp
uid: weblogic_wcp
```

2. Provision the user in the LDAP directory.

   For example, for an Oracle Unified Directory LDAP provider:

```
OUD_INSTANCE_HOME/bin/ldapmodify -a \
                                 -h oudhost.example.com
                                 -D "cn=oudadmin" \
                                 -w password \
                                 -p 1389 \
                                 -f admin_user.ldif
```

   For Oracle Internet Directory:

```
OID_ORACLE_HOME/bin/ldapadd -h oidhost.example.com \
                            -p 3060 \
                            -D cn="orcladmin" \
                            -w password \
                            -c \
                            -v \
                            -f admin_user.ldif
```

3. Create an `ldif` file named `admin_group.ldif` with the contents shown below and then save the file:

```
dn: cn=WCPAdministrators,cn=Groups,dc=example,dc=com
changetype: add
objectclass: top
objectclass: groupOfUniqueNames
objectclass: orclGroup
uniquemember: cn=weblogic_wcp,cn=users,dc=example,dc=com
cn: WCPAdministrators
```

```
displayname: WCPAdministrators
description: Administrators Group for the Oracle WebCenter Portal Domain
```

4. Provision the group in the LDAP Directory.

   For Oracle Unified Directory:

```
OUD_INSTANCE_HOME/bin/ldapmodify -a \
                                 -D "cn=oudadmin" \
                                 -h oudhost.example.com \
                                 -w password \
                                 -p 1380 \
                                 -f admin_group.ldif
```

   For Oracle Internet Directory:

```
OID_ORACLE_HOME/bin/ldapadd -h oid.example.com \
                            -p 3060 \
                            -D cn="orcladmin" \
                            -w password \
                            -c \
                            -v \
                            -f admin_group.ldif
```

5. Verify that the changes were made successfully:

   a. Log in to the Oracle WebLogic Server Administration Console.

   b. In the left pane of the console, click **Security Realms**.

   c. Click the default security realm (**myrealm**).

   d. Click the **Users and Groups** tab.

   e. Verify that the administrator user and group you provisioned are listed on the page.

## 10.9.7 Adding the New Administration User to the Administration Group

After adding the users and groups to Oracle Internet Directory, the group must be assigned the Administration role within the WebLogic domain security realm. This enables all users that belong to the group to be administrators for the domain.

To assign the Administration role to the new enterprise deployment administration group:

1. Log in to the WebLogic Administration Server Console using the administration credentials that you provided in the Configuration Wizard.

   Do not use the credentials for the administration user you created and provided for the new authentication provider.

2. In the left pane of the Administration Console, click **Security Realms**.

3. Click the default security realm (**myrealm**).

4. Click the **Roles and Policies** tab.

5. Expand the **Global Roles** entry in the table and click **Roles**.


6. Click the **Admin** role.


7. Click **Add conditions**.

8. Select **Group** from the **Predicate List** drop-down menu, and then click **Next**.

9. Enter `WCPAdministrators` in the **Group Argument Name** field, and then click **Add**.

   `WCPAdministrators` is added to the list box of arguments.

10. Click **Finish** to return to the Edit Global Role page.

    The `WCPAdministrators` group is now listed.

11. Click **Save** to finish adding the **Admin** Role to the `WCPAdministrators` group.

12. Validate that the changes were made by logging in to the WebLogic Administration Server Console using the new `weblogic_wcp` user credentials.

    If you can log in to the Oracle WebLogic Server Administration Console and Fusion Middleware Control with the credentials of the new administration user you just provisioned in the new authentication provider, then you have configured the provider successfully.

## 10.9.8 Updating the boot.properties File and Restarting the System

After you create the new administration user and group, you must update the Administration Server `boot.properties` file with the administration user credentials that you created in the LDAP directory:

1. On WCPHOST1, go the following directory:

   *ASERVER_HOME*`/servers/AdminServer/security`

2. Rename the existing `boot.properties` file:

   ```
   mv boot.properties boot.properties.backup
   ```

3. Use a text editor to create a file called `boot.properties` under the security directory.

4. Enter the following lines in the file:

   ```
   username=weblogic_wcp
   password=password
   ```

5. Save the file.

6. Restart the Administration Server.

## 10.10 Adding the wsm-pm Role to the Administrators Group

After you configure a new LDAP-based Authorization Provider and restart the Administration Server, add the enterprise deployment administration LDAP group (`WCPAdministrators`) as a member to the `policy.Updater` role in the `wsm-pm` application stripe.

1. Use the Oracle WebLogic Server Administration Server credentials to log in to Oracle Enterprise Manager Fusion Middleware Control.

   These are the credentials you created when you initially configured the domain and created the Oracle WebLogic Server Administration user name (typically, `weblogic_wcp`) and password.

2. From the **WebLogic Domain** menu, select **Security**, and then **Application Roles**.

3. For the `policy.Updater` role, select the `wsm-pm` application stripe from the **Application Stripe** drop-down menu.

4. Click Search Application Roles icon to display all the application roles available in the domain.

5. Select the row for the `policy.Updater` role you are adding to the enterprise deployment administration group.

6. Click the Edit icon to edit the role.

7. Click the Add icon on the Edit Application Role page.

8. In the Add Principal dialog box, select **Group** from the **Type** drop-down menu.

9. Search for the enterprise deployment administrators group, by entering the group name `WCPAdministrators` in the **Principal Name Starts With** field and clicking the right arrow to start the search.

10. Select the administrator group in the search results and click **OK**.

11. Click **OK** on the Edit Application Role page.

## 10.11 Configuring the WebLogic Proxy Plug-In

Before you can validate that requests are routed correctly through the Oracle HTTP Server instances, you must set the `WebLogic Plug-In Enabled` parameter for the clusters you just configured.

1. Log in to the Oracle WebLogic Server Administration Console.

2. In the **Domain Structure** pane, expand the **Environment** node.
3. Click **Clusters**.
4. Select the cluster to which you want to proxy requests from Oracle HTTP Server.

   The **Configuration: General** tab is displayed.
5. Scroll down to the **Advanced** section and expand it.
6. Click **Lock & Edit** in the Change Center.
7. Set **WebLogic Plug-In Enabled** to **yes**.
8. Click **Save** and click **Activate Changes**.
9. Click **Activate Changes** in the Change Center.
10. Restart all Managed Servers in all of the clusters that you modified in this chapter.

# 11

# Configuring the Web Tier for an Enterprise Deployment

It is important to understand how to install and configure a standalone Oracle HTTP Server domain that contains two Oracle HTTP Server instances: one on WEBHOST1 and one on WEBHOST2.

This chapter provides information on variables used when configuring the web tier and installing and configuring a web tier domain.

Variables Used When Configuring the Web Tier
: While configuring the web tier, you will be referencing the directory variables listed in this section.

About the Web Tier Domains
: In an enterprise deployment, each Oracle HTTP Server instance is configured on a separate host and in its own standalone domain. This allows for a simple configuration that requires a minimum amount of configuration and a minimum amount of resources to run and maintain.

Installing Oracle HTTP Server on WEBHOST1
: The following sections describe how to install the Oracle HTTP Server software on the web tier.

Creating a Web Tier Domain on WEBHOST1
: It is essential to understand how to create a new Oracle HTTP Server standalone domain on the first Web tier host.

Installing and Configuring a Web Tier Domain on WEBHOST2
: After you install Oracle HTTP Server and configure a Web Tier domain on WEBHOST1, then you must also perform the same tasks on WEBHOST2.

Starting the Node Manager and Oracle HTTP Server Instances on WEBHOST1 and WEBHOST2
: The following sections describe how to start the Oracle HTTP Server instances on WEBHOST1 and WEBHOST2.

Configuring Oracle HTTP Server to Route Requests to the Application Tier
: The following sections describe how to update the Oracle HTTP Server configuration files so the web server instances route requests to the servers in the domain.

## 11.1 Variables Used When Configuring the Web Tier

While configuring the web tier, you will be referencing the directory variables listed in this section.

The values for several directory variables are defined in File System and Directory Variables Used in This Guide.

- *OHS_ORACLE_HOME*
- *OHS_DOMAIN_HOME*

In addition, you'll be referencing the following virtual IP (VIP) address and host names:

- ADMINVHN
- WEBHOST1
- WEBHOST2

## 11.2 About the Web Tier Domains

In an enterprise deployment, each Oracle HTTP Server instance is configured on a separate host and in its own standalone domain. This allows for a simple configuration that requires a minimum amount of configuration and a minimum amount of resources to run and maintain.

For more information about the role and configuration of the Oracle HTTP Server instances in the web tier, see Understanding the Web Tier.

## 11.3 Installing Oracle HTTP Server on WEBHOST1

The following sections describe how to install the Oracle HTTP Server software on the web tier.



### 11.3.1 Starting the Installer on WEBHOST1

To start the installation program, perform the following steps.

1. Log in to WEBHOST1.
2. Go to the directory in which you downloaded the installation program.
3. Launch the installation program by entering the following command:

   ```
   ./fmw_12.2.1.0.0_ohs_linux64.bin
   ```

   When the installation program appears, you are ready to begin the installation.

### 11.3.2 Navigating the Oracle HTTP Server Installation Screens

The following table lists the screens in the order that the installation program displays them.

If you need additional help with any of the installation screens, click the screen name.

| Screen | Description |
|---|---|
| Welcome | This screen introduces you to the product installer. |
| Auto Updates | Use this screen to automatically search My Oracle Support for available patches or automatically search a local directory for patches that you've already downloaded for your organization. |
| Installation Location | Use this screen to specify the location of your Oracle home directory.<br>For the purposes of an enterprise deployment, enter the value of the OHS_ORACLE_HOME variable listed in Table 7-3. |
| Installation Type | Select **Standalone HTTP Server (Managed independently of WebLogic server)**.<br>This installation type allows you to configure the Oracle HTTP Server instances independently from any other existing Oracle WebLogic Server domains. |
| Prerequisite Checks | This screen verifies that your system meets the minimum necessary requirements.<br>If there are any warning or error messages, verify that your host computers and the required software meet the system requirements and certification information described in Host Computer Hardware Requirements and Operating System Requirements for the Enterprise Deployment Topology. |
| Security Updates | If you already have an Oracle Support account, use this screen to indicate how you would like to receive security updates.<br>If you do not have an account, or if you are sure you want to skip this step, then clear the check box and verify your selection in the follow-up dialog box. |
| Installation Summary | Use this screen to verify the installation options you selected. If you want to save these options to a response file, click **Save Response File** and provide the location and name of the response file. Response files can be used later in a silent installation situation.<br>For more information about silent or command line installation, see "Using the Oracle Universal Installer in Silent Mode" in *Installing Software with the Oracle Universal Installer*. |
| Installation Progress | This screen allows you to see the progress of the installation. |
| Installation Complete | This screen appears when the installation is complete. Review the information on this screen, then click **Finish** to dismiss the installer. |

### 11.3.3 Verifying the Oracle HTTP Server Installation

To verify that your Oracle HTTP Server installation completed successfully, list files that were installed in the new Oracle home directory. You should see the following directories in the Oracle HTTP Server Oracle home:

```
ldap
ohs
css
srvm
has
crs
nls
oracore
precomp
rdbms
plsql
jlib
slax
sqlplus
xdk
oracle_common
webgate
bin
wlserver
OPatch
plugins
oui
perl
network
lib
oraInst.loc
install
cfgtoollogs
inventory
root.sh
```

## 11.4 Creating a Web Tier Domain on WEBHOST1

It is essential to understand how to create a new Oracle HTTP Server standalone domain on the first Web tier host.

Starting the Configuration Wizard on WEBHOST1

Navigating the Configuration Wizard Screens for a Web Tier Domain

### 11.4.1 Starting the Configuration Wizard on WEBHOST1

To start the Configuration Wizard, navigate to the following directory and start the WebLogic Server Configuration Wizard, as follows:

```
cd OHS_ORACLE_HOME/oracle_common/common/bin
./config.sh
```

### 11.4.2 Navigating the Configuration Wizard Screens for a Web Tier Domain

Oracle recommends that you create a standalone domain for the Oracle HTTP Server instances on each Web tier host.

The following topics describe how to create a new standalone Oracle HTTP Server domain:

- Task 1, "Selecting the Domain Type and Domain Home Location"
- Task 2, "Selecting the Configuration Templates"
- Task 3, "Selecting the JDK for the Web Tier Domain."
- Task 4, "Configuring System Components"
- Task 5, "OHS Server Screen"
- Task 7, "Reviewing Your Configuration Specifications and Configuring the Domain"
- Task 8, "Writing Down Your Domain Home"

### Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Create a new domain**.

In the **Domain Location** field, enter the value assigned to the OHS_DOMAIN_HOME variable.

Note the following:

- The Configuration Wizard will create the new directory that you specify here.
- Create the directory on local storage, so the web servers do not have any dependencies on on storage devices outside the DMZ.

### Task 2 Selecting the Configuration Templates

On the Templates screen, select **Oracle HTTP Server (Standalone) - 12.2.1.0.0 [ohs]**.

> **Tip:**
> More information about the options on this screen can be found in "Templates" in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 3 Selecting the JDK for the Web Tier Domain.

Select the Oracle Hotspot JDK, which was installed in the Web tier Oracle home when you installed the Oracle HTTP Server software.

### Task 4 Configuring System Components

On the System Components screen, configure one Oracle HTTP Server instance. The screen should by default have a single instance defined. This is the only instance you need to create.

1. Note that the default instance name is `ohs1` in the **System Component** field. You use this default name.
2. Make sure `OHS` is selected in the **Component Type** field.
3. Use the **Restart Interval Seconds** field to specify the number of seconds to wait before attempting a restart if an application is not responding.

4. Use the **Restart Delay Seconds** field to specify the number of seconds to wait between restart attempts.

### Task 5 OHS Server Screen

Use the OHS Server screen to configure the OHS servers in your domain:

1. Select **ohs1** from the **System Component** drop-down menu.
2. In the **Listen Address** field, enter `WEBHOST1`.

   All of the remaining fields are pre-populated, but you can change the values as required for your organization. For more information about the fields on this screen, see "OHS Server" in *Creating WebLogic Domains Using the Configuration Wizard*.
3. In the **Server Name** field, verify the value of the listen address and listen port.

   It should appear as follows:

   ```
   http://WEBHOST1:7777
   ```

### Task 6 Configuring Node Manager

Select **Per Domain Default Location** as the Node Manager type, and specify the Node Manager credentials.

---

**Note:**
More information about the options on this screen can be found in "Node Manager" in *Creating Domains Using the Configuration Wizard*.

More information about the Node Manager types can be found in "Node Manager Overview" in *Administering Node Manager for Oracle WebLogic Server*.

---

### Task 7 Reviewing Your Configuration Specifications and Configuring the Domain

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation will not begin until you click **Create**.

**Tip:**
More information about the options on this screen can be found in "Configuration Summary" in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 8 Writing Down Your Domain Home

The Configuration Success screen will show the domain home location.

Make a note of the information provided here, as you will need it to start the servers and access the Administration Server.

Click **Finish** to dismiss the configuration wizard.

## 11.5 Installing and Configuring a Web Tier Domain on WEBHOST2

After you install Oracle HTTP Server and configure a Web Tier domain on WEBHOST1, then you must also perform the same tasks on WEBHOST2.

1. Log in to WEBHOST2 and install Oracle HTTP Server, using the instructions in Installing Oracle HTTP Server on WEBHOST1.
2. Configure a new standalone domain on WEBHOST2, using the instructions in Creating a Web Tier Domain on WEBHOST1.

   Use the name `ohs2` for the instance on WEBHOST2, and be sure to replace all occurrences of WEBHOST1 with WEBHOST2 and all occurrences of `ohs1` with `ohs2` in each of the examples.

## 11.6 Starting the Node Manager and Oracle HTTP Server Instances on WEBHOST1 and WEBHOST2

The following sections describe how to start the Oracle HTTP Server instances on WEBHOST1 and WEBHOST2.



### 11.6.1 Starting the Node Manager on WEBHOST1 and WEBHOST2

Before you can start the Oracle HTTP Server instances, you must start the Node Manager on WEBHOST1 and WEBHOST2:

1. Log in to WEBHOST1 and navigate to the following directory:

   ```
   OHS_DOMAIN_HOME/bin
   ```

2. Start the Node Manager as shown below, using `nohup` and `nodemanager.out` as an example output file:

   ```
   nohup OHS_DOMAIN_HOME/bin/startNodeManager.sh > OHS_DOMAIN_HOME/nodemanager/
   nodemanager.out 2>&1 &
   ```

3. Log in to WEBHOST2 and perform steps 1 and 2.

For more information about additional Node Manager configuration options, see *Administering Node Manager for Oracle WebLogic Server*.

### 11.6.2 Starting the Oracle HTTP Server Instances

To start the Oracle HTTP Server instances:

1. Navigate to the following directory on WEBHOST1:

   ```
   OHS_DOMAIN_HOME/bin
   ```

   For more information about the location of the OHS_DOMAIN_HOME directory, see File System and Directory Variables Used in This Guide.

2. Enter the following command:

```
./startComponent.sh ohs1
```

3. When prompted, enter the Node Manager password.

4. Repeat steps 1 through 3 to start the `ohs2` instance on WEBHOST2.

For more information, see "Starting Oracle HTTP Server Instances" in *Administering Oracle HTTP Server*.

## 11.7 Configuring Oracle HTTP Server to Route Requests to the Application Tier

The following sections describe how to update the Oracle HTTP Server configuration files so the web server instances route requests to the servers in the domain.



### 11.7.1 About the Oracle HTTP Server Configuration for an Enterprise Deployment

The following topics provide overview information about the changes required to the Oracle HTTP Server configuration in an enterprise deployment.



#### 11.7.1.1 Purpose of the Oracle HTTP Server Virtual Hosts

The reference topologies in this guide require that you define a set of virtual servers on the hardware load balancer. You can then configure Oracle HTTP Server to recognize requests to specific virtual hosts (that map to the load balancer virtual servers) by adding `<VirtualHost>` directives to the Oracle HTTP Server instance configuration files.

For each Oracle HTTP Server virtual host, you define a set of specific URLs (or context strings) that route requests from the load balancer through the Oracle HTTP Server instances to the appropriate Administration Server or Managed Server in the Oracle WebLogic Server domain.

#### 11.7.1.2 About the WebLogicCluster Parameter of the <VirtualHost> Directive

A key parameter of the Oracle HTTP Server `<VirtualHost>` directive is the `WebLogicCluster` parameter, which is part of the WebLogic Proxy Plug-In for

Oracle HTTP Server. When configuring Oracle HTTP Server for an enterprise deployment, consider the following information when adding this parameter to the Oracle HTTP Server configuration files.

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. The listed cluster member must be running when Oracle HTTP Server is started. Oracle WebLogic Server and the plug-in work together to update the server list automatically with new, failed, and recovered cluster members.

Some example scenarios:

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

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

#### 11.7.1.3 Recommended Structure of the Oracle HTTP Server Configuration Files

Rather than adding multiple virtual host definitions to the `httpd.conf` file, Oracle recommends that you create separate, smaller, and more specific configuration files for each of the virtual servers required for the products you are deploying. This avoids populating an already large `httpd.conf` file with additional content, and it can make troubleshooting configuration problems easier.

For example, in a typical Oracle Fusion Middleware Infrastructure domain, you can add a specific configuration file called `admin_vh.conf` that contains the virtual host definition for the Administration Server virtual host (ADMINVHN).

### 11.7.2 Modifying the httpd.conf File to Include Virtual Host Configuration Files

Perform the following tasks to prepare the `httpd.conf` file for the additional virtual hosts required for an enterprise topology:

1. Log in to WEBHOST1.
2. Locate the `httpd.conf` file for the first Oracle HTTP Server instance (`ohs1`) in the domain directory:

   ```
   cd OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/
   ```

3. Open the `httpd.conf` file in a text editor and make the following changes:

   a. Create a `ServerName` entry in the Virtual Hosts section of the httpd.conf file, below the `# Virtual Hosts` comment block and before the `# VirtualHost Example`: comment as follows:

   ```
   ##### Virtual hosts ######

   # Virtual Hosts
   #
   ```

```
# If you want to maintain multiple domains/hostnames on your
# machine you can setup VirtualHost containers for them. Most configurations
# use only name-based virtual hosts so the server doesn't need to worry
about
# IP addresses. This is indicated by the asterisks in the directives below.
#
# Please see the documentation at
# URL
# for further details before you try to setup virtual hosts.

ServerName http://WEBHOST1:7777

#
# VirtualHost example:
```

In this example, replace WEBHOST1 with the value of the WEBHOST1 variable. For more information, see File System and Directory Variables Used in This Guide.

**b.** Verify that there is an `INCLUDE` statement in the `httpd.conf` that includes all `*.conf` files in the `moduleconf` subdirectory:

```
IncludeOptional "moduleconf/*.conf"
```

This statement makes it possible to create the separate virtual host files for each component, making it easier to update, maintain, and scale out the virtual host definitions.

4. Save the `httpd.conf` file.
5. Log in to WEBHOST2 and perform steps 2 through 4 to update the `httpd.conf` file for the `ohs2` instance.

   On WEBHOST2, replace all instances of WEBHOST1 with WEBHOST2 and all instances of `ohs1` with `ohs2`.

## 11.7.3 Creating the Virtual Host Configuration Files

To create the virtual host configuration files:

> **Note:** Before you create the virtual host configuration files, be sure you have configured the virtual servers on the load balancer, as described in Purpose of the Oracle HTTP Server Virtual Hosts.

1. Log in to WEBHOST1 and change directory to the configuration directory for the first Oracle HTTP Server instance (`ohs1`):

   ```
   cd OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf
   ```

2. Create the `admin_vh.conf` file and add the following directive:

   ```
   <VirtualHost WEBHOST1:7777>
       ServerName admin.example.com:80
       ServerAdmin you@your.address
       RewriteEngine On
       RewriteOptions inherit
   </VirtualHost>
   ```

3. Create the `wcpinternal_vh.conf` file and add the following directive:

```
<VirtualHost WEBHOST1:7777>
    ServerName wcpinternal.example.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit
</VirtualHost>
```

4. Restart the `ohs1` instance:

   a. Change directory to the following location:

      ```
      cd OHS_DOMAIN_HOME/bin
      ```

   b. Enter the following commands to stop and start the instance; provide the node manager password when prompted:

      ```
      ./stopComponent.sh ohs1
      ./startComponent.sh ohs1
      ```

5. Copy the `admin_vh.conf` file and the `wcpinternal_vh.conf` file to the configuration directory for the second Oracle HTTP Server instance (`ohs2`) on WEBHOST2:

   ```
   OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs2/moduleconf
   ```

6. Edit the `admin_vh.conf` and `wcpinternal_vh.conf` files and change any references from WEBHOST1 to WEBHOST2 in the `<VirtualHost>` directives.

7. Restart the `ohs2` instance:

   a. Change directory to the following location:

      ```
      cd OHS_DOMAIN_HOME/bin
      ```

   b. Enter the following commands to stop and start the instance:

      ```
      ./stopComponent.sh ohs2
      ./startComponent.sh ohs2
      ```

### 11.7.4 Validating the Virtual Server Configuration on the Load Balancer

From the load balancer, access the following URLs to ensure that your load balancer and Oracle HTTP Server are configured properly. These URLs should show the initial Oracle HTTP Server 12*c* web page.

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

### 11.7.5 Configuring Routing to the Administration Server and Oracle Web Services Manager

To enable Oracle HTTP Server to route to the Administration Server and the WSM-PM_Cluster, which contain the WLS_WSM managed servers, you must add a set of `<Location>` directives and add the `WebLogicCluster` parameter to the list of nodes in the cluster.

To set the `WebLogicCluster` parameter:

1. Log in to WEBHOST1, and change directory to the following location:

```
cd OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf/
```

2. Add the following directives to the `admin_vh.conf` file within the `<VirtualHost>` tags:

```
# Admin Server and EM
<Location /console>
    WLSRequest ON
    WebLogicHost ADMINVHN
    WeblogicPort 7001
</Location>

<Location /consolehelp>
    WLSRequest ON
    WebLogicHost ADMINVHN
    WeblogicPort 7001
</Location>

<Location /em>
    WLSRequest ON
    WebLogicHost ADMINVHN
    WeblogicPort 7001
</Location>
```

   The `admin_vh.conf` file should appear as it does in Example 1, "admin_vh.conf file".

3. Add the following directives to the `wcpinternal_vh.conf` file within the `<VirtualHost>` tag:

```
# WSM-PM
<Location /wsm-pm>
    WLSRequest ON
    WebLogicCluster WCPHOST1:7010,WCPHOST2:7010
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>
```

   The `wcpinternal_vh.conf` file should appear as it does in Example 2, "wcpinternal_vh.conf file".

   For more information about the WebLogicCluster parameter in this example, see About the WebLogicCluster Parameter of the <VirtualHost> Directive.

4. Restart the ohs1 instance:

   a. Change directory to the following location:

      ```
      cd OHS_DOMAIN_HOME/bin
      ```

   b. Enter the following commands to stop and start the instance:

      ```
      ./stopComponent.sh ohs1
      ./startComponent.sh ohs1
      ```

5. Copy the `admin_vh.conf` file and the `wcpinternal_vh.conf` file to the configuration directory for the second Oracle HTTP Server instance (ohs2) on WEBHOST2:

   *OHS_DOMAIN_HOME*`/config/fmwconfig/components/OHS/`**`ohs2`**`/moduleconf/`

6. Edit the `admin_vh.conf` and `wcpinternal_vh.conf` files and change any references to WEBHOST1 to WEBHOST2 in the `<VirtualHost>` directives.

7. Restart the ohs2 instance:

   a. Change directory to the following location:

      ```
      cd OHS_DOMAIN_HOME/bin
      ```

   b. Enter the following commands to stop and start the instance:

      ```
      ./stopComponent.sh ohs2
      ./startComponent.sh ohs2
      ```

**Example 1 admin_vh.conf file**

```
<VirtualHost WEBHOST1:7777>
    ServerName admin.example.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit

# Admin Server and EM
<Location /console>
    WLSRequest ON
    WebLogicHost ADMINVHN
    WeblogicPort 7001
</Location>

<Location /consolehelp>
    WLSRequest ON
    WebLogicHost ADMINVHN
    WeblogicPort 7001
</Location>

<Location /em>
    WLSRequest ON
    WebLogicHost ADMINVHN
    WeblogicPort 7001
</Location>
</VirtualHost>
```

**Example 2 `wcpinternal_vh.conf` file**

Contents of this file:

```
<VirtualHost WEBHOST1:7777>
    ServerName wcpinternal.example.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit

# WSM-PM
<Location /wsm-pm>
    WLSRequest ON
    WebLogicCluster WCPHOST1:7010,WCPHOST2:7010
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
```

```
</Location>
</VirtualHost>
```

### 11.7.6 Validating Access to the Management Consoles and Administration Server

To verify the changes you have made in this chapter:

1. Use the following URL to the hardware load balancer to display the Oracle WebLogic Server Administration Console, and log in using the Oracle WebLogic Server administrator credentials:

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

   This validates that the `admin.example.com` virtual host on the load balancer is able to route requests to the Oracle HTTP Server instances on the web tier, which in turn can route requests for the Oracle WebLogic Server Administration Console to the Administration Server in the application tier.

2. Similarly, you should be able to access the Fusion Middleware Control using a similar URL:

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

### 11.7.7 Validating Access to the Oracle Web Services Policy Manager

To verify that the Oracle HTTP Server virtual host and load-balancer for the internal URLs are configured correctly, also verify the WSM-PM configuration:

Use the following URL for the hardware load balancer to display the Oracle Web Services Policy Manager web interface, and log in using the Oracle WebLogic server administrator credentials.

```
http://wcpinternal.example.com/wsm-pm
```

# 12

# Extending the Domain with Oracle WebCenter Portal

The following topics describes how to extend the enterprise deployment domain with the Oracle WebCenter Portal software.

Variables Used When Extending the Domain for WebCenter Portal

Installing the Software for an Enterprise Deployment
The following sections describe how to install the software for an enterprise deployment.

Creating the Oracle WebCenter Portal Database Schemas

Extending the Enterprise Deployment Domain with Oracle WebCenter Portal

Propagating the Extended Domain to the Domain Directories and Machines

Restarting and Validating Pre-existing Managed Servers

Modifying the Upload and Stage Directories to an Absolute Path
After configuring the domain and unpacking it to the Managed Server domain directories on all the hosts, verify and update the `upload` and `stage` directories for the new Managed Servers.

Starting and Validating the WC_Portal1, WC_Portlet1, WC_Collaboration1 Managed Servers

Configuring Analytics

Configuring REST APIs
This section describes the procedure to configure REST APIs.

Modifying System Configuration MBean Values for the WebCenter Portal Content Manager Component

Configuring Oracle HTTP Server for the Extended Domain
The following sections describe how to configure the Oracle HTTP Server instances so they route requests for both public and internal URLs to the proper clusters in the enterprise topology.

Configuring WebCenter Portal for External Services

## 12.1 Variables Used When Extending the Domain for WebCenter Portal

As you perform the tasks in this chapter, you will be referencing the following directory variables, which are defined in File System and Directory Variables Used in This Guide.

- ORACLE_HOME

- ASERVER_HOME
- APPLICATION_HOME
- DEPLOY_HOME
- OHS_CONFIG_DIR
- JAVA_HOME

In addition, you'll be referencing the following virtual IP (VIP) addresses and host names defined in Physical and Virtual IP Addresses Required by the Enterprise Topology:

- ADMINVHN
- WCPHOST1
- WCPHOST2
- DBHOST1
- DBHOST2
- SCAN Address for the Oracle RAC Database (DB-SCAN.examle.com)

## 12.2 Installing the Software for an Enterprise Deployment

The following sections describe how to install the software for an enterprise deployment.

Starting the Oracle WebCenter Portal Installer on WCPHOST1

Navigating the Installation Screens

Installing Oracle WebCenter Portal on the Other Host Computers

### 12.2.1 Starting the Oracle WebCenter Portal Installer on WCPHOST1

To start the installation program:

1. Log in to WCPHOST1.
2. Go to the directory where you downloaded the installation program.
3. Launch the installation program by invoking the `java` executable from the JDK directory on your system, as shown in the example below.

   ```
   JAVA_HOME/bin/java -d64 -jar fmw_12.2.1.0.0_wcportal_generic.jar
   ```

   Be sure to replace the JDK location in these examples with the actual JDK location on your system.

   For information about downloading the software and locating the actual installer file name for your product, see Identifying and Obtaining Software Downloads for an Enterprise Deployment.

When the installation program appears, you are ready to begin the installation.

### 12.2.2 Navigating the Installation Screens

The installation program displays a series of screens, in the order listed in the following table.

If you need additional help with any of the installation screens, click the screen name.

| Screen | Description |
|---|---|
| Welcome | This screen introduces you to the product installer. |
| Auto Updates | Use this screen to automatically search My Oracle Support for available patches or automatically search a local directory for patches that you've already downloaded for your organization. |
| Installation Location | Use this screen to specify the location of your Oracle home directory.<br>For more information about Oracle Fusion Middleware directory structure, see "Selecting Directories for Installation and Configuration" in *Planning an Installation of Oracle Fusion Middleware*. |
| Installation Type | Use this screen to select the type of installation and consequently, the products and feature sets you want to install.<br>Select **WebCenter Portal**.<br>**Notes:**<br>• WebCenter Portal Worklist integration requires that the BPEL Services provided by SOA Suite share the same WebTier, SSO, and Identity Store.<br>• For this Enterprise Deployment Guide, SOA Suite is installed and configured in the same WebLogic Server Domain and included in the WebTier, SSO, and Directory configurations.<br>• Whether the installation has SOA Suite installed in the same or separate `ORACLE_HOME`, the WebCenter Portal SOA Composites option is required as a separate installation. For instructions about the installation see, Installing the Oracle WebCenter Portal SOA Composites. |
| Prerequisite Checks | This screen verifies that your system meets the minimum necessary requirements.<br>If there are any warning or error messages, you can refer to one of the following documents in the Roadmap for Verifying Your System Environment section in *Planning Your Oracle Fusion Middleware Infrastructure Installation.* |
| Security Updates | If you already have an Oracle Support account, use this screen to indicate how you would like to receive security updates.<br>If you do not have one and are sure you want to skip this step, clear the check box and verify your selection in the follow-up dialog box. |
| Installation Summary | Use this screen to verify the installation options you selected.<br>Click **Install** to begin the installation. |

| Screen | Description |
|---|---|
| Installation Progress | This screen allows you to see the progress of the installation.<br>Click **Next** when the progress bar reaches 100% complete. |
| Installation Complete | Review the information on this screen, then click **Finish** to dismiss the installer. |

### 12.2.3 Installing Oracle WebCenter Portal on the Other Host Computers

If you have followed the EDG shared storage recommendations, there is a separate shared storage volume for product installations on WCPHOST2, and you must also install the software on WCPHOST2. For more information, see Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment.

## 12.3 Creating the Oracle WebCenter Portal Database Schemas

Before you can configure an Oracle WebCenter Portal domain, you must install the required schemas on a certified database for use with this release of Oracle Fusion Middleware.

The following topics describe how to install the required schemas.



### 12.3.1 Starting the Repository Creation Utility (RCU)

To start the Repository Creation Utility (RCU):

1. Navigate to the *ORACLE_HOME*`/oracle_common/bin` directory on your system.
2. Make sure the *JAVA_HOME* environment variable is set to the location of a certified JDK on your system. The location should be up to but not including the `bin` directory. For example, if your JDK is located in `/u01/oracle/products/jdk`:

   On UNIX operating systems:

   ```
   export JAVA_HOME=/u01/oracle/products/jdk
   ```

3. Start RCU:

   On UNIX operating systems:

   ```
   ./rcu
   ```

### 12.3.2 Navigating the RCU Screens to Create the Schemas

Schema creation involves the following tasks.

**Task 1 Introducing RCU**
Click **Next**.

### Task 2 Selecting a Method of Schema Creation

If you have the necessary permission and privileges to perform DBA activities on your database, select **System Load and Product Load**. This procedure assumes that you have the necessary privileges.

If you do not have the necessary permission or privileges to perform DBA activities in the database, you must select **Prepare Scripts for System Load** on this screen. This option will generate a SQL script, which can be provided to your database administrator. See "Understanding System Load and Product Load" in *Creating Schemas with the Repository Creation Utility*.

### Task 3 Providing Database Connection Details

Provide the database connection details for RCU to connect to your database.

In the **Host Name** field, enter the SCAN address of the Oracle RAC Database.

Enter the **DBMS/Service** details.

Enter the **Schema Owner** and **Schema Password** details.

Click **Next** to proceed, then click **OK** on the dialog window confirming that connection to the database was successful.

### Task 4 Specifying a Custom Prefix and Selecting Schemas

Select **Select existing prefix**, and then select the prefix you used when you created the initial domain in Creating the Initial Infrastructure Domain for an Enterprise Deployment.

From the list of schemas, select **WebCenter Portal** . This will automatically select the required WebCenter Portal schemas. In addition, the following dependent schemas have already been installed with the Infrastructure and are grayed out:

- Metadata Services
- Audit Services
- Audit Services Append
- Audit Services Viewer
- Oracle Platform Security Services
- User Messaging Service

The custom prefix is used to logically group these schemas together for use in this domain only; you must create a unique set of schemas for each domain as schema sharing across domains is not supported.

> **Tip:**
> For more information about custom prefixes, see "Understanding Custom Prefixes" in *Creating Schemas with the Repository Creation Utility*.
>
> For more information about how to organize your schemas in a multi-domain environment, see "Planning Your Schema Creation" in *Creating Schemas with the Repository Creation Utility*.

Click **Next** to proceed, then click **OK** on the dialog window confirming that prerequisite checking for schema creation was successful.

**Task 5 Specifying Schema Passwords**

Specify how you want to set the schema passwords on your database, then specify and confirm your passwords.

> **Tip:**
> You must make a note of the passwords you set on this screen; you will need them later on during the domain creation process.

**Task 6 Specifying Custom Variables**

For an enterprise deployment, Oracle recommends that you enter "Y" to enable partitioning of the Analytics data.

This feature partitions the analytics data by month. In a partitioned environment, the recommended method for purging data is simply to drop the month-based partitions that are no longer required.

For information about partitioning analytics data, see "Partitioning Oracle WebCenter Portal's Analytics Data" in the *Oracle Fusion Middleware Administrator's Guide*.

**Task 7 Verifying the Tablespaces for the Required Schemas**

On the Map Tablespaces screen, review the information, and then click **Next** to accept the default values.

Click **OK** in the confirmation dialog box.

**Task 8 Completing Schema Creation**

Navigate through the remainder of the RCU screens to complete schema creation. When you reach the Completion Summary screen, click **Close** to dismiss RCU.

**Task 9 Verifying the Schema Creation**

To verify that the schemas were created successfully, and to verify the database connection details, use SQL*Plus or another utility to connect to the database, using the WCPINFRA schema name and the password you provided.

For example:

```
./sqlplus

SQL*Plus: Release 11.2.0.4.0 Production on Fri Nov 1 08:44:18 2013

Copyright (c) 1982, 2013, Oracle.  All rights reserved.

Enter user-name: FMW1221_WEBCENTER
Enter password: wcpinfra_password

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL>
```

# 12.4 Extending the Enterprise Deployment Domain with Oracle WebCenter Portal

This section provides instructions for extending the existing enterprise deployment domain with the Oracle WebCenter Portal software.

Extending the domain involves the following:

Starting the Configuration Wizard

Navigating the Configuration Wizard Screens to Extend the Domain with WebCenter Portal

## 12.4.1 Starting the Configuration Wizard

To start the Configuration Wizard:

1. Shut down the domain completely before extending the domain. From the WebLogic Server Console, stop all managed servers and verify, and then stop the Administration Server.
2. Navigate to the following directory and start the WebLogic Server Configuration Wizard.

```
cd ORACLE_HOME/oracle_common/common/bin
./config.sh
```

## 12.4.2 Navigating the Configuration Wizard Screens to Extend the Domain with WebCenter Portal

Follow the instructions in this section to update and configure the domain for the topology.

---

**Note:**

If your needs do not match the instructions given in the procedure, be sure to make your selections accordingly, or refer to the supporting documentation for additional details.

---

Domain configuration includes the following tasks.

**Task 1 Selecting the Domain Type and Domain Home Location**

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the ASERVER_HOME variable, which represents the complete path to the Administration Server domain home you created in Creating the Initial Infrastructure Domain for an Enterprise Deployment.

For more information about the directory location variables, see File System and Directory Variables Used in This Guide

**Tip:**
More information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle WebCenter Portal – 12.2.1.1.0 [wcportal]**
- **Oracle WebCenter Pagelet Producer – 12.2.1.1.0 [wcportal]**
- **Oracle WebCenter Portlet Producers - 12.2.1.1.0 [wcportal]**
- **Oracle WebCenter Discussion Server - 12.2.1.1.0 [wcportal]**
- **Oracle WebCenter Analytics Collector - 12.2.1.1.0 [wcportal]**

In addition, the following additional templates should already be selected, because they were used to create the initial domain in Creating the Initial Infrastructure Domain for an Enterprise Deployment:

- **Oracle Enterprise Manager - 12.2.1.1.0 [em]**
- **Oracle WSM Policy Manager - 12.2.1.0 [oracle_common]**
- **Oracle JRF - 12.2.1.1.0 [oracle_common]**
- **WebLogic Coherence Cluster Extension - 12.2.1.1.0 [wlserver]**

**Tip:**
More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 3 Specifying the Database Configuration Type

On the Database Configuration Type screen, select **RCU Data**.

All fields are pre-populated, because you already configured the domain to reference the Fusion Middleware schemas that are required for the Infrastructure domain.

Verify and ensure that credentials in all the fields are the same that you have provided while configuring Oracle Fusion Middleware Infrastructure.

Click **Get RCU Configuration** after you finish verifying the database connection information. The following output in the Connection Result Log indicates that the operation succeeded:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK

Successfully Done.
```

**Tip:**
For more information about the **RCU Data** option, see "Understanding the Service Table Schema" in *Creating Schemas with the Repository Creation Utility*.

For more information about the other options on this screen, see "Datasource Defaults" in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 4 Specifying JDBC Component Schema Information

On the JDBC Component Schema screen, select all the WebCenter Portal schemas in the table.

When you select the schemas, the fields on the page are activated and the database connection fields are populated automatically.

Click **Convert to GridLink** and click **Next**.

### Task 5 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, provide the information required to connect to the RAC database and component schemas, as shown in the following table.

| Element | Description and Recommended Value |
|---|---|
| SCAN, Host Name, and Port | Select the **SCAN** check box.<br>In the **Host Name** field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database.<br>In the **Port** field, enter the SCAN listening port for the database (for example, `1521`) |
| ONS Host and Port | In the **ONS Host** field, enter the SCAN address for the Oracle RAC database.<br>In the **Port** field, enter the ONS Remote port (typically, `6200`). |
| Enable Fan | Select the **Enable Fan** check box to receive and process FAN events, |

### Task 6 Testing the JDBC Connections

Use the JDBC Component Schema Test screen to test the data source connections you have just configured.

A green check mark in the Status column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

**Tip:**
For more information about the other options on this screen, see "Test Component Schema" in *Creating WebLogic Domains Using the Configuration Wizard*

### Task 7 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

- Topology
- Deployments and Services

**Task 8 Configuring Managed Servers**

On the Managed Servers screen, new Managed Servers for Oracle WebCenter Portal, Portlets, and Collaboration appear in the list of servers along with the other Managed Servers that were created earlier. These servers are created automatically by the Oracle WebCenter Portal configuration template you selected earlier in the Configuration Wizard session.

Perform the following tasks to modify the default Managed Servers and create a second Managed Server for each server type:

1. Select WC_Portal and rename it to WC_Portal1.
2. Select **Clone** to create another managed server. Rename the new server to WC_Portal2.
3. Repeat the above two steps to edit and create WC_Portlet1, WC_Portlet2, WC_Collaboration1 and WC_Collaboration2.

**Tip:**
More information about the options on the Managed Server screen can be found in Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

| Server Name | Listen Address | Listen Port | Enable SSL | SSL Listen Port | Server Groups |
|---|---|---|---|---|---|
| WLS_WSM1 | WCPHOST1 | 7010 | No | Disabled | WSMPM-MAN-SVR<br>JRF-MAN-SVR<br>WSM-CACHE-SVR |
| WLS_WSM2 | WCPHOST2 | 7010 | No | Disabled | WSMPM-MAN-SVR<br>JRF-MAN-SVR<br>WSM-CACHE-SVR |
| WC_Portal1 | WCPHOST1 | 9001 | No | Disabled | WebCenter Portal Managed Server<br>WebCenter Portal Analytics Managed Server |
| WC_Portal2 | WCPHOST2 | 9001 | No | Disabled | WebCenter Portal Managed Server<br>WebCenter Portal Analytics Managed Server |
| WC_Portlet1 | WCPHOST1 | 9002 | No | Disabled | WebCenter Portal Pagelet Producer Managed Server<br>WebCenter Portal Portlet Producer Managed Server |
| WC_Portlet2 | WCPHOST2 | 9002 | No | Disabled | WebCenter Portal Pagelet Producer Managed Server<br>WebCenter Portal Portlet Producer Managed Server |

| Server Name | Listen Address | Listen Port | Enable SSL | SSL Listen Port | Server Groups |
|---|---|---|---|---|---|
| WC_Collaboration1 | WCPHOST1 | 9003 | No | Disabled | WebCenter Portal Discussions Managed Server |
| WC_Collaboration2 | WCPHOST2 | 9003 | No | Disabled | WebCenter Portal Discussions Managed Server |

**Task 9 Configuring a Cluster**

In the Configure Clusters screen, add three new clusters:

- Portal_Cluster
- Portlet_Cluster
- Collab_Cluster

For all three clusters, leave the default values for **Cluster Address**, **Frontend Host**, and **Port**.

**Note:**
By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to "Considerations for Choosing Unicast or Multicast" in *Administering Clusters for Oracle WebLogic Server*.

**Tip:**
More information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 10 Assigning Managed Servers to the Cluster**

Use the Assign Servers to Clusters screen to assign Managed Servers to their respective cluster:

1. In the Clusters pane, select the cluster to which you want to assign the servers; in this case, `Portal_Cluster`.
2. In the Servers pane, assign WC_Portal1 to `Portal_Cluster` by doing one of the following:
   - Click once on `WC_Portal1` Managed Server to select it, then click on the right arrow to move it beneath the selected cluster in the Clusters pane.
   - Double-click on `WC_Portal1` to move it beneath the selected cluster in the clusters pane.
3. Repeat to assign `WC_Portal2` to `Portal_Cluster`.
4. Repeat steps 1-3 to assign `WC_Portlet1` and `WC_Portlet2` to `Portlet_Cluster`.
5. Repeat steps 1-3 to assign `WC_Collaboration1` and `WC_Collaboration2` to `Collaboration_Cluster`.

**Tip:**
More information about the options on this screen can be found in Assign Servers to Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 11 Configuring Coherence Clusters**
Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at 9991, as it was defined during the initial Infrastructure domain creation.

**Note:**
For Coherence licensing information, refer to "Oracle Coherence" in *Oracle Fusion Middleware Licensing Information*.

**Task 12 Verifying the Existing Machines**
Under the Unix Machine tab, verify the names of the machines you created when creating the initial Infrastructure domain.

Click Next to proceed.

**Task 13 Assigning Servers to Machines**
Use the Assign Servers to Machines screen to assign the Managed Servers you just created to the corresponding machines in the domain.

Assign `WC_Portal1`, `WC_Portlet1`, `WC_Collaboration1` to `WCPHOST1`.

Assign `WC_Portal2`, `WC_Portlet2`, `WC_Collaboration2` to `WCPHOST2`.

**Tip:**
More information about the options on this screen can be found in Assign Servers to Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 14 Creating Virtual Targets**
Click **Next** to proceed to the next screen.

**Task 15 Creating Partitions**
Click **Next** to proceed to the next screen.

**Task 16 Deployments Targeting**
With the Oracle Web Services Manager Policy Manager deployed to a separate cluster, the default targeting of the WSM-PM application to the Portal, Collaboration, and Portlet clusters can be removed.

For each of the Portal_Cluster, Collaboration_Cluster, and Portlet_Cluster in the Targets panel:

Select the wsm-pm application entry within the Application folder and click the left arrow button to remove it from the targets list.

**Task 17 Services Targeting**
With the Oracle Web Services Manager Policy Manager deployed to a separate cluster, the default targeting of the WSM-PM service resources to the Portal, Collaboration, and Portlet clusters can be removed.

For each of the Portal_Cluster, Collaboration_Cluster, and Portlet_Cluster in the Targets panel:

Select and remove the following two resources from the targets list:

- mds-owsm
- WSM Startup Class

**Task 18 Reviewing Your Configuration Specifications and Configuring the Domain**
The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation will not begin until you click **Update**.

> **Tip:**
> More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 19 Writing Down Your Domain Home and Administration Server URL**
The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server.

Click **Finish** to dismiss the configuration wizard.

**Task 20 Start the Administration Server**
Start the Administration Server to ensure the changes you have made to the domain have been applied.

## 12.5 Propagating the Extended Domain to the Domain Directories and Machines

After you have extended the domain with the Oracle WebCenter Portal instances, and you have started the Administration Server on WCPHOST1, you must then propagate the domain changes to the domain directories and machines.

1. Create a copy of the Managed Server domain directory and the Managed Server `applications` directory.
2. Run the following `pack` command on WCPHOST1 to create a template pack:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true
          -domain=ASERVER_HOME
          -template=/full_path/wcpdomaintemplateExtWCP.jar
          -template_name=wcpdomain_templateExtWCP
```

   In this example:

   - Replace *ASERVER_HOME* with the actual path to the domain directory you created on the shared storage device.
   - Replace *full_path* with the complete path to the directory where you want the template jar file saved.
   - `wcpdomaintemplateExtWCP.jar` is a sample name for the JAR file you are creating, which will contain the domain configuration files, including the configuration files for the Oracle HTTP Server instances.
   - `wcpdomain_templateExtWCP` is the name assigned to the domain template file.

3. Run the following `unpack` command on WCPHOST1 to propagate the template created in the preceding step to the *MSERVER_HOME* directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME
            -template=/full_path/wcpdomaintemplateExtWCP.jar
            -app_dir=APPLICATION_HOME
            -overwrite_domain=true
```

   In this example:

   - Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
   - `wcpdomaintemplateExtWCP.jar`is the directory path and name of the template you created when you ran the pack command to pack up the domain on the shared storage device.
   - The `-overwrite_domain=true` argument is necessary when you are 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.
   - Replace *`APPLICATION_HOME`* with the complete path to the Application directory for the domain on local storage.

**Tip:**

For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

4. Run the following command on WCPHOST1 to copy the template pack created in step 1 to WCPHOST2:

```
scp /full_path/wcpdomaintemplateExtWCP.jar oracle@WCPHOST2:/full_path/
```

5. Run the following `unpack` command on WCPHOST2 to deploy the domain template copied in the preceding step to the local *MSERVER_HOME* domain directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME
            -template=/full_path/wcpdomaintemplateWCP.jar
            -app_dir=APPLICATION_HOME
            -overwrite_domain=true
```

In this example:

- Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
- `wcpdomaintemplateWCP.jar`is the directory path and name of the template you created when you ran the pack command to pack up the domain on the shared storage device.
- The `-overwrite_domain=true` argument is necessary when you are 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.
- Replace *`APPLICATION_HOME`* with the complete path to the Application directory for the domain on local storage.

**Tip:**

For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

## 12.6 Restarting and Validating Pre-existing Managed Servers

Restart the managed servers for the pre-existing components now that the domain has been extended and unpacked to the *MSERVER_HOME* directories on all of the servers.

1. From the WebLogic Server Console, restart the WLS_WSM*n* Managed Servers for the WebServices Manager Policy Manager.

2. From another browser window, verify the WSM-PM application is responding by successfully loading the URL:

   ```
   http://wcpinternal.example.com/wsm-pm/validator
   ```

## 12.7 Modifying the Upload and Stage Directories to an Absolute Path

After configuring the domain and unpacking it to the Managed Server domain directories on all the hosts, verify and update the `upload` and `stage` directories for the new Managed Servers.

This step is necessary to avoid potential issues when performing remote deployments and for deployments that require the stage mode.

To update these directory paths for all the Managed Servers in the Managed Server domain home directory:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the left navigation tree, expand **Domain**, and then **Environment**.
3. Click **Lock & Edit**.
4. Click **Servers**.
5. For each new Managed Server in the Managed Server domain home directory:
   a. Click the name of the Managed Server.
   b. Click the **Configuration** tab, and then click the **Deployment** tab.
   c. Verify that the **Staging Directory Name** is set to the following:

      ```
      MSERVER_HOME/servers/server_name/stage
      ```

      Replace *MSERVER_HOME* with the directory path for the MSERVER_HOME directory; replace *server_name* with the name of the Server you are editing.

   d. Update the **Upload Directory Name** to the following value:

      ```
      ASERVER_HOME/servers/AdminServer/upload
      ```

      Replace *ASERVER_HOME* with the directory path for the ASERVER_HOME directory.

   e. Click **Save**.
   f. Return to the Summary of Servers screen.
6. When you have modified these values for each Managed Server, click **Activate Changes**.

## 12.8 Starting and Validating the WC_Portal1, WC_Portlet1, WC_Collaboration1 Managed Servers

Now that you have extended the domain, restarted the Administration Server, and propagated the domain to the other hosts, you can start the newly configured Oracle WebCenter Portal servers.

This process involves three tasks:

## 12.8.1 Starting the Managed Servers on WCPHOST1

To start the WC_Portal1 Managed Server:

1. Enter the following URL into a browser to display the Fusion Middleware Control login screen:

   `http://ADMINVHN:7001/em`

2. Log in to Fusion Middleware Control using the Administration Server credentials.

3. In the **Target Navigation** pane, expand the domain to view the Managed Servers in the domain.

4. Select only the **WC_Portal1** Managed Server and click **Start Up** on the Oracle WebLogic Server toolbar.

   **Note:**

   WebCenter Portal Servers depend on the policy access service to be functional. This implies that the WSM-PM Managed Servers in the domain need to be up and running and reachable before the WebCenter Portal servers are started.

5. When the startup operation is complete, navigate to the Domain home page and verify that the WC_Portal1 Managed Server is up and running.

6. Repeat the above steps to start the WC_Portlet1 and WC_Collaboration1 Managed Servers on WCPHOST1.

## 12.8.2 Adding the WCPAdmin Role to the Portal Administrators Group

Before you validate the Oracle WebCenter Portal configuration on WC_Portal1 Managed Server, grant the WebCenter Portal administrator role to the `WCPAdministrators` LDAP group.

To perform this task, refer to Configuring Roles for Administration of Oracle WebCenter Portal Products.



### 12.8.2.1 Granting the Administrator Role for WebCenter Portal Using WLST

To grant the WebCenter Portal Administrator role using WLST:

1. Create a group in the LDAP store named **WCPAdministrators**.

   This group will be assigned the Administrator role in WebCenter Portal.

   For more information on how to create a user, see Provisioning an Enterprise Deployment Administration User and Group and Adding the New Administration User to the Administration Group.

2. Navigate to your WebCenter Portal Oracle home directory and invoke the WLST script:

   ```
   (UNIX) MW_HOME/wc/common/bin/wlst.sh

   (Windows) MW_HOME\wc\common\bin\wlst.cmd
   ```

3. Connect to the Administration Server for the target domain with the following command:

   ```
   wls:/offline>connect("user_name","password", "host_name:port_number")
   ```

4. Grant the WebCenter Portal Administrator application role to the WCPAdministrators group in LDAP using the `grantAppRole` command.

   ```
   grantAppRole(appStripe="webcenter",
   appRoleName="s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator",
   principalClass="weblogic.security.principal.WLSGroupImpl",
   principalName="WCPAdministrators")
   ```

   Where **WCPAdministrators** is the name of the portal administration group you created earlier.

5. Restart the `WC_Portal1` Managed Server.

   ```
   shutdown('WC_Portal1', block='true', force='true')
   start('WC_Portal1', block='true')
   ```

6. To test the new account, log in to WebCenter Portal using the new account name.

   Open WebCenter Portal in your browser using `http://WCPHOST1:9001/webcenter`. After logging in, the **Administration** link should appear, and you should be able to perform all administrative operations.

#### 12.8.2.2 Granting the Administrator Role for WebCenter Portal Using Fusion Middleware Control

This section describes how to grant WebCenter Portal's **Administrator** role to a user account other than the default **weblogic** account.

To grant WebCenter Portal's Administrator role using Fusion Middleware Control:

1. Log into Fusion Middleware Control as `weblogic_wcp` and navigate to the home page for WebCenter Portal.

**Note:**

When administering WebCenter resources in the Enterprise Manager Fusion Middleware Control, it is recommended to use the WebCenter-specific administrative user created in LDAP (for example, weblogic_wcp). For more information, see Adding the New Administration User to the Administration Group.

2. Expand the **Target Navigation** panel by clicking on the button with the four grey horizontal lines in the top-left of the Enterprise Manager screen.
3. Navigate to the portal instance status view. Expand the **WebCenter** > **Portal** > **Server** navigation elements. Click on the first portal instance listed (for example, **WebCenter Portal (WC_Portal1)**).
4. From the WebCenter Portal menu, select **Security**, and then select **Application Roles**.

   The Application Roles page displays.
5. Search for WebCenter Portal's Administrator role:
   a. Change the search form's Role Name option from **Starts With** to **Includes**.
   b. In the text box next to the **Includes** option, enter `#Administrator`, then click the blue search (arrow) icon.
6. Click the returned row to select the Administrators role.
7. Click the **Edit** menu option to open the Edit Application Role view.
8. Click the **Add** menu option.

   The form to add members is displayed.
9. Change the search type from **Application Role** to **Group**.
10. Use the Search function to search for the **WCPAdministrators** LDAP group created earlier in Provisioning an Enterprise Deployment Administration User and Group.
11. Click to select the correct row of search results for the **WCPAdministrators** group.
12. Click **OK** to add the selected group to the role.
13. On the **Edit Application Role** page, verify the updated list of members includes the newly added group.
14. Click **OK** to save the changes to the Application Role.
15. Restart the **WC_Portal1** Managed Server.

    When you log in to WebCenter Portal as a member of the WCPAdministrators group, the Administration link should appear and you should be able to perform all administrative operations.

#### 12.8.2.3 Granting the Administration Role for WebCenter Discussions using WLST

The WCPAdministrators LDAP group also needs to be granted an administrative role for the WebCenter Portal Discussions Services. Use the WLST commands listed here to apply that role grant for the LDAP group.

1. Navigate to your WebCenter Portal Oracle home directory and invoke the WLST script:

   ```
   (Unix) ORACLE_COMMON_HOME/common/bin/wlst.sh
   (Windows) ORACLE_COMMON_HOME/common/bin/wlst.cmd
   ```

2. Connect to the Administration Server for the target domain with the following command:

   ```
   wls:/offline>connect("user_name","password", "ADMINVHN:7001")
   ```

3. Grant the Discussions Administrator privileges to the WCPAdministrators LDAP group using the `addDiscussionsServerAdmin` command.

   ```
   addDiscussionsServerAdmin(appName='owc_discussions', server='WC_Collaboration1',
   name='WCPAdministrators', type='GROUP')
   ```

   Where WCPAdministrators is the name of the portal administration group you created earlier.

4. Restart the Collab_Cluster via WLST.

   ```
   shutdown('WC_Collaboration1', block='true', force='true')
   start('WC_Collaboration1', block='true')
   ```

5. To test the new account, log in to WebCenter Discussions Admin using the weblogic_wcp account name. Open WebCenter Discussions administration application in your browser using `http://WCPHOST1:9003/owc_discussions/admin`. If you can log in, the grant was successful.

### 12.8.3 Starting and Validating the Managed Servers on WCPHOST2

After you have validated the successful configuration and startup of the Managed Servers on WCPHOST1, you can then start and validate the new Managed Servers on WCPHOST2, using the procedure in Starting and Validating the WC_Portal1, WC_Portlet1, WC_Collaboration1 Managed Servers.

For the validation URL, enter the following in your Web browser and log in using the enterprise deployment administration user (`weblogic_wcp`):

```
http://WCPHOST2:9001/webcenter/
```

## 12.9 Configuring Analytics

Out-of-the box, analytics collectors are configured to communicate with the local WebCenter Portal application in a 1-1 relationship (the collectors listen on localhost). No additional analytics collector configuration is required.

However, you must configure the WebCenter Portal applications to send event messages to localhost:

**Note:** Clustered analytics collectors are not supported for collecting WebCenter Portal events.

To connect the WebCenter Portal application to the analytics collector:

1. Connect to the Managed Server where the WebCenter Portal application is running using WLST, for example:

   ```
   ORACLE_COMMON_HOME/common/bin/wlst.sh
   connect("weblogic_admin_username", "weblogic_admin_pwd", "t3://ADMINVHN:7001")
   ```

   Connect to the host and port of the WC_Portal server.

2. Create a connection between the WebCenter Portal application and the analytics collector and make it the default connection (default=1).

   **Note:**

   The commands in this section need to be executed only once for the clustered Webcenter application, even though there is a specific server name listed for the connection. When this configuration is set, it applies to all servers.

   For example:

   ```
   createAnalyticsCollectorConnection(appName="webcenter", server="WC_Portal1",
   connectionName="Collector31314", isUnicast=1, collectorHost="localhost",
   collectorPort=31314, isEnabled=1, timeout=30, default=1)
   ```

   See also, the **createAnalyticsCollectorConnection** section in the *WebLogic Scripting Tool Command Reference*.

3. Verify the changes made:

   ```
   listDefaultAnalyticsCollectorConnection(appName="webcenter", server="WC_Portal1")
   ```

   See also the **listDefaultAnalyticsCollectorConnection** section in the *WebLogic Scripting Tool Command Reference*.

## 12.10 Configuring REST APIs

This section describes the procedure to configure REST APIs.

If you want to use WebCenter Portal REST APIs, confirm the server-side credential store configuration by executing the commands described in this section.

These credential entries should already be configured as part of the domain extension for WebCenter Portal.

To confirm the seed entries in the credential store that enable the REST security tokens to function properly, execute these WLST commands:

**Note:** If the credential maps already exist, JPS-01007 exceptions messages will be returned. This confirms the configuration.

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

```
ORACLE_COMMON_HOME/common/bin/wlst.sh
connect('weblogic_admin_username','weblogic_admin_pwd','t3://ADMINVHN:7001')
```

2. Run the following WLST commands to configure the credential store:

```
createCred(map="o.webcenter.jf.csf.map", key="keygen.algorithm",
     user="keygen.algorithm", password="AES")
createCred(map="o.webcenter.jf.csf.map", key="cipher.transformation",
     user="cipher.transformation", password="AES/CBC/PKCS5Padding")
```

Later on, you must configure REST policies in OAM.

## 12.11 Modifying System Configuration MBean Values for the WebCenter Portal Content Manager Component

The WebCenter Portal Content Manager component and task flows utilize the WebCenter Content remote UI (RUI) APIs to provide content integration capabilities. While these libraries are directly included with the Portal installation, specific MBean configuration settings need to be modified for fail-safe runtime within a High Availability architecture.

Modify and validate the following attributes for the `ADFConfig:WccAdfConfiguration` and `ADFConfig:ADFcConfig` application-defined MBeans on the portal application:

- ADFConfig:ADFcConfig:
  - AdfScopeHaSupport
- ADFConfig:WccAdfConfiguration:
  - ClusterCompatible
  - TemporayDirectory

The upload temporary directory specified must be configured to a common directory location on a shared disk volume across all portal nodes when the portal is clustered in a High Availability environment.

1. Create a unique folder on the ORACLE_RUNTIME shared volume for the Portal Content Manager component upload location.

   ```
   mkdir -p ORACLE_RUNTIME/DOMAIN_NAME/Portal_Cluster/wccAdfUpload
   ```

   For example,

   ```
   mkdir -p /u01/oracle/runtime/wcedg/Portal_Cluster/wccAdfUpload
   ```

2. Log in to Fusion Middleware Control as `weblogic_wcp`.
3. From the WebLogic Domain menu, select **System MBean Browser**.
4. Under Application Defined MBeans, navigate to the WccAdfConfiguration attribute: **oracle.adf.share.config** > **Server: WC_Portal1** > **Application: webcenter** > **ADFConfig** > **ADFConfig** >**ADFConfig** > **WccAdfConfiguration**

> **Note:** This MBean value only needs to be set once from any of the portal server instances and will apply to all.

5. Set the `ClusterCompatible` attribute to a value of: `true`.
6. Set the Temporary Directory attribute to the directory created above on shared storage.

   The Temporary Directory attribute must be set to a directory so that the uploaded files stored under that directory can be accessed by both WCPHOST1 and WCPHOST2.

   For example,

   ```
   /u01/oracle/runtime/wcedg/Portal_Cluster/wccAdfUpload
   ```

7. Under Application Defined MBeans, navigate to the **ADFcConfiguration** attribute: **oracle.adf.share.config** > **Server: WC_Portal1** > **Application: webcenter** > **ADFConfig** > **ADFConfig** >**ADFConfig** > **ADFcConfiguration**.
8. Verify the `AdfScopeHASupport` attribute value is set to true, update if necessary, then click **apply** if an update is required.
9. Click **Apply** and verify that a confirmation message appears at the top of the page.
10. Navigate to the adf-config MBean to invoke the save operation. Click oracle.adf.share.config > Server: WC_Portal1 > Application: webcenter > ADFConfig > ADFConfig
11. Click the **Operations** tab.
12. Click **Save Operation**.
13. On the Operation:save page, click **Invoke** to commit all the MBean changes made since the last save operation. Verify a confirmation message appears at the top of the page.
14. Restart all managed servers in the portal cluster.

## 12.12 Configuring Oracle HTTP Server for the Extended Domain

The following sections describe how to configure the Oracle HTTP Server instances so they route requests for both public and internal URLs to the proper clusters in the enterprise topology.



### 12.12.1 Configuring Oracle HTTP Server for the Oracle WebCenter Portal Clusters

To configure the Oracle HTTP Server instances in the Web tier so they route requests correctly to the Oracle WebCenter Portal clusters, use the following procedure to create an additional Oracle HTTP Server configuration file that creates and defines the parameters of the `wcp.example.com` virtual server.

This procedure assumes you performed the Oracle HTTP Server configuration tasks described in Configuring Oracle HTTP Server to Route Requests to the Application Tier.

To create the virtual host configuration file so requests are routed properly:

1. Log in to WEBHOST1 and change directory to the configuration directory for the first Oracle HTTP Server instance (OHS1):

   ```
   cd OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf/
   ```

2. Create the `wcp_vh.conf` file and add the following directive:

   ```
   <VirtualHost WEBHOST1:7777>
       ServerName https://wcp.example.com:443
       ServerAdmin you@your.address
       RewriteEngine On
       RewriteOptions inherit
   </VirtualHost>
   ```

3. Add the following directives inside the `<VirtualHost>` tags:

   ```
   # WebCenter Portal Application (previously called Spaces)
   <Location /webcenter>
       WLSRequest ON
       WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
       WLProxySSL ON
       WLProxySSLPassThrough ON
   </Location>

   <Location /webcenterhelp>
       WLSRequest ON
       WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
       WLProxySSL ON
       WLProxySSLPassThrough ON
   </Location>

   <Location /rss>
       WLSRequest ON
       WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
       WLProxySSL ON
       WLProxySSLPassThrough ON
   </Location>

   <Location /rest>
       WLSRequest ON
       WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
       WLProxySSL ON
       WLProxySSLPassThrough ON
   </Location>

   # Discussions
   <Location /owc_discussions>
       WLSRequest ON
       WebLogicCluster WCPHOST1:9003,WCPHOST2:9003
       WLProxySSL ON
       WLProxySSLPassThrough ON
   </Location>

   <Location /portalTools>
       WLSRequest ON
       WebLogicCluster WCPHOST1:9002,WCPHOST2:9002
   ```

```
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

<Location /wsrp-tools>
    WLSRequest ON
    WebLogicCluster WCPHOST1:9002,WCPHOST2:9002
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

</VirtualHost>
```

4. Copy the `wcp_vh.conf` file into the configuration directory for the second Oracle HTTP Server instance (ohs2) on WEBHOST2:

```
scp OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf/wcp_vh.conf \
WEBHOST2:/OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs2/moduleconf/
wcp_vh.conf
```

5. Log in to WEBHOST2 and change directory to the configuration directory for the second Oracle HTTP Server instance (ohs2):

```
cd OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs2/moduleconf/
```

6. Edit the `wcp_vh.conf` and change any references to WEBHOST1 to WEBHOST2 in the `<VirtualHost>` directives.

7. Restart both Oracle HTTP servers.

## 12.12.2 Configuring the WebLogic Proxy Plug-In

Before you can validate that requests are routed correctly through the Oracle HTTP Server instances, you must set the `WebLogic Plug-In Enabled` parameter for the clusters you just configured.

1. Log in to the Oracle WebLogic Server Administration Console.

2. In the **Domain Structure** pane, expand the **Environment** node.

3. Click **Clusters**.

4. Select the cluster to which you want to proxy requests from Oracle HTTP Server.

   The **Configuration: General** tab is displayed.

5. Scroll down to the **Advanced** section and expand it.

6. Click **Lock & Edit** in the Change Center.

7. Set **WebLogic Plug-In Enabled** to **yes**.

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

9. Click **Activate Changes** in the Change Center.

10. Restart all Managed Servers in all of the clusters that you modified in this chapter.

### 12.12.3 Validating the Oracle WebCenter Portal Public Services URLs Through the Load Balancer

To validate the configuration of the Oracle HTTP Server virtual hosts and to verify that the hardware load balancer can route public service requests through the Oracle HTTP Server instances to the application tier:

1. 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.

2. Verify that you can access these URLs:

   - `https://wcp.example.com/rss`
   - `https://wcp.example.com/rest/api/resourceIndex`
   - `https://wcp.example.com/portalTools`
   - `https://wcp.example.com/wsrp-tools`
   - `https://wcp.example.com/owc_discussions`

### 12.12.4 Configuring HTTP Server for Internal WebCenter Services

To configure the Oracle HTTP Server instances in the Web tier so they route requests correctly to the internal Oracle WebCenter services, use the following procedure to edit existing `wcpinternal_vh.conf` file.

This procedure assumes you performed the Oracle HTTP Server configuration tasks described in Configuring Oracle HTTP Server to Route Requests to the Application Tier.

To edit the virtual host configuration file so requests are routed properly:

1. Log in to WEBHOST1 and change directory to the configuration directory for the first Oracle HTTP Server instance (ohs1):

   ```
   cd OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf/
   ```

2. Edit the `wcpinternal_vh.conf` file and add the following directives near the end of the file just above the last line: `</VirtualHost>`

   ```
   # WebCenter Portal Application Services

   <Location /webcenter>
       WLSRequest ON
       WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
       WLProxySSL OFF
       WLProxySSLPassThrough OFF
   </Location>

   <Location /webcenterhelp>
       WLSRequest ON
       WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
       WLProxySSL OFF
       WLProxySSLPassThrough OFF
   ```

```
</Location>

<Location /rss>
    WLSRequest ON
    WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

<Location /rsscrawl>
    WLSRequest ON
    WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

<Location /sesUserAuth>
    WLSRequest ON
    WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

<Location /rest>
    WLSRequest ON
    WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# Discussions
<Location /owc_discussions>
    WLSRequest ON
    WebLogicCluster WCPHOST1:9003,WCPHOST2:9003
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# Portlets
<Location /pagelets>
    WLSRequest ON
    WebLogicCluster WCPHOST1:9002,WCPHOST2:9002
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

<Location /portalTools>
    WLSRequest ON
    WebLogicCluster WCPHOST1:9002,WCPHOST2:9002
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

<Location /wsrp-tools>
    WLSRequest ON
    WebLogicCluster WCPHOST1:9002,WCPHOST2:9002
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# Collector
```

```
<Location /collector>
    WLSRequest ON
    WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

</VirtualHost>
```

3. Copy the `wcpinternal_vh.conf` file into the configuration directory for the second Oracle HTTP Server instance (ohs2) on WEBHOST2:

```
scp OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf/
wcpinternal_vh.conf \
WEBHOST2:/OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs2/moduleconf/
wcpinternal_vh.conf
```

4. Log in to WEBHOST2 and change directory to the configuration directory for the second Oracle HTTP Server instance (ohs2):

```
cd OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs2/moduleconf/
```

5. Edit the `wcpinternal_vh.conf` file and change any references from WEBHOST1 to WEBHOST2 in the `<VirtualHost>` directives.

6. Restart both Oracle HTTP servers.

### 12.12.5 Validating the Oracle WebCenter Portal Internal Services URLs Through the Load Balancer

To validate the configuration of the Oracle HTTP Server virtual hosts and to verify that the hardware load balancer can route internal service requests through the Oracle HTTP Server instances to the application tier:

1. 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.

2. Verify that you can access these URLs:

   - `http://wcpinternal.example.com/rss`
   - `http://wcpinternal.example.com/rest/api/resourceIndex`
   - `http://wcpinternal.example.com/pagelets`
   - `http://wcpinternal.example.com/portalTools`
   - `http://wcpinternal.example.com/wsrp-tools`
   - `http://wcpinternal.example.com/owc_discussions`

## 12.13 Configuring WebCenter Portal for External Services

This section describes how to configure external tools and services for WebCenter Portal applications using Fusion Middleware Control or WLST commands. For most

external services, you must set up a connection between the WebCenter Portal application and the backend server.

Configuring Default Web Service Policies for WebCenter Portal, Discussions, and Portlet Producer Applications

Configuring the Discussions Server Connection

Registering Portlet Producers

Registering the Pagelet Producer

Configuring Search Services

Configuring Oracle WebCenter Portal Notifications for the SMTP Mail Server

## 12.13.1 Configuring Default Web Service Policies for WebCenter Portal, Discussions, and Portlet Producer Applications

After installing Oracle WebCenter Portal, you must attach the default Oracle Web Services Manager (OWSM) security policy to the following:

- WebCenter Portal application (webcenter)
- Discussions application (owc_discussions)
- WebCenter Services Portlet Producer (services-producer)
- WSRP Tools Producer (wsrp-tools)

These steps are required because security policies for these Web service end points are not configured out-of-the-box.

To attach the default Web service security policy:

1. Ensure that `WC_Portal1`, `WC_Portal2`, `WC_Collaboration1`, `WC_Collaboration2`, `WC_Portlet1`, and `WC_Portlet2` managed servers are up and running.
2. Start the WebLogic Scripting Tool:

   ```
   WCPHOST1> ORACLE_COMMON_HOME/common/bin/wlst.sh
   ```

3. Connect to the Administration Server as an administrator.

   For example

   ```
   connect("weblogic_wcp","admin password","t3://ADMINVHN:7001")
   ```

   For information, see the "Running Oracle WebLogic Scripting Tool (WLST) Commands" section in **Oracle Fusion Middleware Administering Oracle WebCenter Portal**.

4. Run WLST commands to attach the default OWSM security policy (oracle/wss10_saml_token_service_policy) to each of the following:
   - WebCenter Portal application (webcenter)
   - Discussions application (owc_discussions)
   - WebCenter Services Portlet Producer (services-producer)

- WSRP Tools Producer (wsrp-tools)

**Note:**

In the examples in this topic, configure the application path with the domain name and managed server names for your environment. The examples below use the domain name *wcedg*.

**a.** To attach the default OWSM security policy to the discussions Web service on each server in the cluster (WC_Collaboration1 and WC_Collaboration2), run the following WLST commands:

```
attachWebServicePolicy(application='/domain_name/WC_Collaboration1/
owc_discussions', moduleName='owc_discussions', moduleType='web',
serviceName='OWCDiscussionsServiceAuthenticated',
subjectName='OWCDiscussionsServiceAuthenticated', policyURI='oracle/
wss10_saml_token_service_policy')
```

**b.** Run the following WLST commands to attach the default OWSM security policy to the WSRP Tools Producer's Web service end point on each server in the cluster (WC_Portlet1 and WC_Portlet2):

```
attachWebServicePolicy(application='/domain_name/WC_Portlet1/wsrp-tools',
moduleName='wsrp-tools', moduleType='web', serviceName='WSRP_v2_Service',
subjectName='WSRP_v2_Markup_Service', policyURI='oracle/
wss10_saml_token_service_policy')
```

5. Restart the `WC_Portal1`, `WC_Portal2`, `WC_Collaboration1`, `WC_Collaboration2`, `WC_Portlet1`, and `WC_Portlet2` managed servers.

## 12.13.2 Configuring the Discussions Server Connection

If you want to provide discussions or announcements in WebCenter Portal, you must connect the application to a discussions server. To configure a connection for the WebCenter Portal Enterprise Deployment, the following values are required:

- Discussions Server URL: **http://wcpinternal.example.com/owc_discussions**
- Discussions Admin User: **WebCenter Portal Admin user name** from LDAP (for example, `weblogic_wcp`)
- Discussions Admin Password: **WebCenter Portal Admin user password**
- Authenticated User Web Service Policy URI: **WSS 1.0 SAML Token Client Policy**

You can connect to a discussions server using Fusion Middleware Control or WLST commands.

For more information, see "Managing Announcements and Discussions" in *Administering Oracle WebCenter Portal*.

Creating a Discussions Server Connection Using Fusion Middleware Control

Creating a Discussions Server Connection using WLST
If you want to use the command line, rather than Fusion Middleware Control, then you can connect your WebCenter Portal application to a discussions server using the WebLogic Scripting Tool.

### 12.13.2.1 Creating a Discussions Server Connection Using Fusion Middleware Control

To connect your WebCenter Portal application to a discussions server using Fusion Middleware Control:

1. Ensure that at least one of the managed servers on which your application is deployed is up and running.

   For example, check one of the WC_Portal managed servers.

2. Log on to the Enterprise Manager Fusion Middleware Control Console at the following URL:

   `http://ADMINVHN:7001/em`

3. Navigate to the home page for your WebCenter Portal application.

   For example, to navigate to the home page for the WebCenter Portal application, open **Target Navigation** and select **WebCenter** > **Portal** > **Server** and then **WebCenter Portal (WC_Portal1)**.

4. From the WebCenter Portal drop-down menu, select **Settings**, and then **Service Configuration**.

5. Click **Discussions and Announcements**, and then **Add**.

6. In the Add Discussion and Announcement Connection screen:

   - **Connection Name**: DFConnection
   - **Active Connection**: Select this check box to enable the connection
   - **Server URL**: `http://wcpinternal.example.com/owc_discussions`
   - **Administrator User Name**: Name of a WebCenter Portal admin user from LDAP (for example, `weblogic_wc`)
   - **Authenticated User Web Service Policy URI:** Select **WSS 1.0 SAML Token Client Policy** (oracle/wss10_saml_token_client_policy)

7. Click **OK** to save the settings.

8. Restart the managed servers on which the application is deployed.

   For the WebCenter Portal application, restart all the managed servers in the Portal_Cluster.

### 12.13.2.2 Creating a Discussions Server Connection using WLST

If you want to use the command line, rather than Fusion Middleware Control, then you can connect your WebCenter Portal application to a discussions server using the WebLogic Scripting Tool.

1. Start the WebLogic Scripting Tool:

   ```
   WCPHOST1> ORACLE_COMMON_HOME/common/bin/wlst.sh
   ```

2. In WLST, connect as the administrator.

   For example:

   ```
   connect("weblogic_wcp","admin password","ADMINVHN:7001")
   ```

3. Use the `createDiscussionForumConnection` command to connect to the discussions server.

   For example:

   ```
   createDiscussionForumConnection(appName="webcenter",name="DFConnection",
   url="http://wcpinternal.example.com/owc_discussions",
   adminUser="weblogic_wcp",default=1,policyURIForAuthAccess="oracle/
   wss10_saml_token_client_policy",server="WC_Portal1")
   ```

   Where **webcenter** is the name of the WebCenter Portal application deployed on WC_Portal1 and weblogic_wc is the name of the discussions server admin user.

   For more information, see "createDiscussionForumConnection" in the *WebCenter WLST Command Reference*.

4. Restart the managed servers on which the application is deployed.

   For the WebCenter Portal application, restart all the managed servers in the Portal_Cluster.

## 12.13.3 Registering Portlet Producers

Several out-of-the-box portlet producers can be registered with the WebCenter Portal application. In the WebCenter Portal Enterprise Deployment, the required producer URLs are as follows:

- WSRP Producer URL: **http://wcpinternal.example.com/wsrp-tools/portlets/wsrp2?WSDL**
- WebClipping Producer URL: **http://wcpinternal.example.com/portalTools/webClipping/providers**
- OmniPortlet Producer URL: **http://wcpinternal.example.com/portalTools/omniPortlet/providers**

You can register portlet producers using Fusion Middleware Control or WLST commands.

Registering Out-of-the-Box Portlet Producers using Fusion Middleware Control

Registering Out-of-the-Box Portlet Producers Using WLST

### 12.13.3.1 Registering Out-of-the-Box Portlet Producers using Fusion Middleware Control

For details on how to register portlet producers using Fusion Middleware Control, see "Managing Portlet Producers" in *Administering Oracle WebCenter Portal*.

#### 12.13.3.2 Registering Out-of-the-Box Portlet Producers Using WLST

To register out-of-the-box portlet producers using WLST:

1. Start the WebLogic Scripting Tool:

   ```
   WCPHOST1> ORACLE_HOME/oracle_common/common/bin/wlst.sh
   ```

2. In WLST, connect as the administrator.

   For example:

   ```
   connect("weblogic_wcp","admin password","t3://ADMINVHN:7001",server="WC_Portal1")
   ```

3. Register all three out-of-the-box WSRP and PDK-Java producers.

   For example:

   ```
   registerOOTBProducers(producerHost='wcpinternal.example.com',producerPort=80,
   appName='webcenter', server='WC_Portal1')
   ```

   Where **webcenter** is the name of the WebCenter Portal application deployed on WC_Portal1.

   See also, "registerOOTBProducers" in the *WebCenter WLST Command Reference*.

### 12.13.4 Registering the Pagelet Producer

If you want to expose WSRP and Oracle JPDK portlets and OpenSocial gadgets as pagelets in WebCenter Portal, you must register the pagelet producer. In the WebCenter Portal Enterprise Deployment, the required pagelet producer URL is:

**http://wcpinternal.example.com/pagelets**

You can register the pagelet producer using Fusion Middleware Control or WLST commands.

Registering Pagelet Producer Using Fusion Middleware Control

Registering Pagelet Producer Using WLST

#### 12.13.4.1 Registering Pagelet Producer Using Fusion Middleware Control

To register Pagelet Producer using Fusion Middleware Control:

1. Log in to Fusion Middleware Control as `weblogic_wcp`, and navigate to the WebCenter Portal home page.

   **Note:**

   When administering WebCenter resources in the Enterprise Manager Fusion Middleware Control, it is recommended to use the WebCenter-specific administrative user created in the remote LDAP authenticator (for example, `weblogic_wcp`). For more information, see Configuring Roles for Administration of an Enterprise Deployment.

   For more information, see “Navigating to the Home page for WebCenter Portal” in *Administering Oracle WebCenter Portal* .

2. From the **WebCenter Portal** menu, select **Register Producer**.
3. Enter connection details for Pagelet Producer, as shown in the following table.

| Field | Description |
|---|---|
| Connection Name | A unique name to identify this Pagelet Producer instance within the application. The name must be unique across all WebCenter Portal connection types. The name specified here appears in Composer under the UI Components > Pagelet Producers folder (by default). |
| Producer Type | Select **Pagelet Producer**. |
| Server URL | The URL to Pagelet Producer. The URL must include a fully-qualified domain name. Use the following syntax:<br>`<protocol>://<host_name>:<port_number>/pagelets/`<br>For example:<br>`http://wcpinternal.example.com/pagelets/`<br>If pagelets contain secure data, the registered URL must use the `https` protocol. For example:<br>`https://wcp.example.com/pagelets/`<br>The context root can be changed from `/pagelets/` if necessary; for details, see "Redeploying Pagelet Producer to a Different Context" in *Administering Oracle WebCenter Portal*.<br>Note: In WebCenter Portal, if the Pagelet Producer URL is protected by OAM, the URL to the pagelet catalog must be excluded (mapped directly without access control), or the catalog will appear to be empty when using REST. The pagelet catalog URL is `http://<host_name>:<port_number>/pagelets/api/v2/ensemble/pagelets` |

4. Click **OK**. The new producer appears in the connection table.

### 12.13.4.2 Registering Pagelet Producer Using WLST

To register out-of-the-box pagelet producers using WLST:

1. Start the WebLogic Scripting Tool:

   ```
   WCPHOST1> ORACLE_COMMON_HOME/common/bin/wlst.sh
   ```

2. In WLST, connect as the administrator.

   For example,

```
connect("weblogic_wcp","admin password","t3://ADMINVHN:
7001",server="WC_Portal1")
```

3. Register the pagelet producer by entering the following command.

```
registerPageletProducer(appName='webcenter',
name='PageletProducer', url='http://wcpinternal.example.com/
pagelets', server='WC_Portal1')
```

For command syntax and examples, see `registerPageletProducer` in *WebCenter WLST Command Reference*.

You can also use WLST to list or edit the current connection details.

For information on how to run WLST commands, see "Running Oracle WebLogic Scripting Tool (WLST) Commands" in *Administering Oracle WebCenter Portal*.

## 12.13.5 Configuring Search Services

You can configure Oracle Secure Enterprise Search (Oracle SES) services and crawlers using procedures in the "Managing Oracle SES Search" section in Oracle Fusion Middleware Administering Oracle WebCenter Portal.

Ensure that:

- Oracle Secure Enterprise Search is registered with Oracle Internet Directory and the WebCenter Portal application is configured as an Oracle SES trusted entity, as described in the "Oracle SES - Configuration" section in Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal.
- Connection exists between the WebCenter Portal application and Oracle Secure Enterprise Search, as described in the "Setting Up Oracle SES Connections" section in Oracle Fusion Middleware Administering Oracle WebCenter Portal.

Ensure that any new URLs are added to the `wcpinternal.example.com` host in the `wcinternal_vh.conf` file as follows:

```
<Location /rsscrawl>
    WLSRequest ON
    WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

<Location /sesUserAuth>
    WLSRequest ON
    WebLogicCluster WCPHOST1:9001,WCPHOST2:9001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>
```

## 12.13.6 Configuring Oracle WebCenter Portal Notifications for the SMTP Mail Server

In a WebCenter Portal Enterprise Deployment, if you choose to send notifications using mail, you must configure a connection to your corporate mail server and specify several unique parameters for the sent emails to appear correctly.

To ensure sufficient configuration for your mail server and business requirements, before completing this task, review Managing Mail in *Administering Oracle WebCenter Portal* for details on the required and optional configurations and parameters.

You can register a mail server using Fusion Middleware Control or WLST commands:

### 12.13.6.1 Registering Mail Servers Using Fusion Middleware Control

For details on how to register a mail server using Fusion Middleware Control, see Registering Mail Servers Using Fusion Middleware Control in *Administering Oracle WebCenter Portal*.

### 12.13.6.2 Registering Mail Servers Using WLST

Use the WLST command `createMailConnection` to create a mail server connection.

1. Start the WebLogic Scripting Tool:

   ```
   ORACLE_HOME/oracle_common/common/bin/wlst.sh
   ```

2. Connect to the Administration Server.

   For example:

   ```
   connect('weblogic_wcp','admin password','t3://ADMINVHN:7001')
   ```

3. Register an External Application Connection for the mail server:

   ```
   createMailExtAppConnection(appName='webcenter', name='CorpMailServer',
   displayName='Corporate Mail Server', server='WC_Portal1')
   ```

4. Register a Mail Server Connection:

   ```
   createMailConnection(appName='webcenter', name='NotificationSharedConn',
   smtpHost='mail.example.com', smtpPort=25, smtpSecured=0,
   timeout=10, default=1,appId='CorpMailServer', server='WC_Portal1')
   ```

   **Note:**

   Additional capabilities are available and might be required depending on your mail server and business needs, such as the ability to notify distribution lists. For more information, see Managing Mail in *Administering Oracle WebCenter Portal*.

5. Set the required mail server connection properties.

   These properties ensure that a specific mail address is the same in the external application and in the mail server. These properties are added to the mail connection and are used by mail for the **From**, **Display Name**, and **Reply To** fields.

   For example:

   ```
   setMailConnectionProperty(appName='webcenter', name='NotificationSharedConn',
   key='mail.user.emailAddress', value='john.doe@example.com')

   setMailConnectionProperty(appName='webcenter', name='NotificationSharedConn',
   key='mail.user.displayName', value='John Doe')

   setMailConnectionProperty(appName='webcenter', name='NotificationSharedConn',
   key='mail.user.replyToAddress', value='feedback@example.com')
   ```

6. **For Exchange 2007 only**, create a universal distribution list. To do this, you must update the value of the `mail.exchange.dl.group.type` property from 2 (default value) to 8.

   Specify a value of 8 for the `mail.exchange.dl.group.type` mail property, as follows:

   ```
   setMailServiceProperty(appName='webcenter',
   property='mail.exchange.dl.group.type', value='8')
   ```

   If your application offers a self-registration page with the facility to mail user ID information on request, then you must ensure that public credentials are configured for the external application selected here. If public credentials are not defined, then mail cannot be sent to users on their request. WebCenter Portal offers this feature on its default self-registration page.

7. Restart the Portal cluster:

   ```
   shutdown('Portal_Cluster', 'Cluster',force='true',block='true')
   start('Portal_Cluster', 'Cluster',block='true')
   ```

# 13

# Extending the Domain to Include Oracle WebCenter Content

This chapter describes how to extend the enterprise deployment domain with the Oracle WebCenter Content software.

This chapter provides information on installing the WebCenter Content, extending the domain for WebCenter Content and completing post-configuration and verification tasks.

Installing WebCenter Content for an Enterprise Deployment
: This section provides instructions for installing WebCenter Content in an enterprise deployment domain.

Creating the Oracle WebCenter Content Database Schemas
: Before you can configure an Oracle WebCenter Content domain, you must install the required schemas in a certified database for use with this release of Oracle Fusion Middleware.

Extending the Domain for WebCenter Content
: This section provides instructions for extending the existing enterprise deployment domain with the Oracle WebCenter Content software.

Completing Postconfiguration and Verification Tasks for WebCenter Content
: Several configuration and validation steps must be performed to bring the content servers online. Complete the following sections in the order listed.

Configuring Oracle HTTP Server for the WebCenter Content Cluster
: The following sections provide instructions for configuring Oracle HTTP Server for the WebCenter Content Cluster.

Configuring Oracle WebCenter Content for WebCenter Portal
: This section describes tasks required for configuring Oracle WebCenter Content Server for use with WebCenter Portal.

Registering Oracle WebCenter Content with the WebCenter Portal Application
: Perform the following steps to register Oracle WebCenter Content Server with the WebCenter Portal application.

## 13.1 Installing WebCenter Content for an Enterprise Deployment

This section provides instructions for installing WebCenter Content in an enterprise deployment domain.

This section contains the following procedures.

Starting the Oracle WebCenter Content Installer on WCPHOST1

Navigating the Installation Screens

Installing Oracle WebCenter Content on the Other Host Computers

Verifying the Installation

### 13.1.1 Starting the Oracle WebCenter Content Installer on WCPHOST1

To start the installation program:

1. Log in to WCPHOST1.
2. Go to the directory where you downloaded the installation program.
3. Launch the installation program by invoking the `java` executable from the JDK directory on your system, as shown in the example below.

   ```
   JAVA_HOME/bin/java -d64 -jar fmw_12.2.1.0.0_wccontent_generic.jar
   ```

   Be sure to replace the JDK location in these examples with the actual JDK location on your system.

   For information about downloading the software and locating the actual installer file name for your product, see Identifying and Obtaining Software Downloads for an Enterprise Deployment.

When the installation program appears, you are ready to begin the installation.

### 13.1.2 Navigating the Installation Screens

The installation program displays a series of screens, in the order listed in the following table.

If you need additional help with any of the installation screens, click the screen name.

| Screen | Description |
|---|---|
| Installation Inventory Screen | If you did not create a central inventory when you installed the Oracle Fusion Middleware Infrastructure software, then this dialog box appears.<br>Edit the **Inventory Directory** field so it points to the location of your local inventory, and then click **OK**. |
| Welcome | This screen introduces you to the product installer. |
| Auto Updates | Use this screen to automatically search My Oracle Support for available patches or automatically search a local directory for patches that you've already downloaded for your organization. |
| Installation Location | Use this screen to specify the location of your Oracle home directory.<br>For more information about Oracle Fusion Middleware directory structure, see "Selecting Directories for Installation and Configuration" in *Planning an Installation of Oracle Fusion Middleware*. |
| Prerequisite Checks | This screen verifies that your system meets the minimum necessary requirements.<br>If there are any warning or error messages, you can refer to one of the documents in the Roadmap for Verifying Your System Environment section in *Planning Your Oracle Fusion Middleware Infrastructure Installation.* |

| Screen | Description |
|---|---|
| Installation Summary | Use this screen to verify the installation options you selected.<br>Click **Install** to begin the installation. |
| Installation Progress | This screen allows you to see the progress of the installation.<br>Click **Next** when the progress bar reaches 100% complete. |
| Installation Complete | Review the information on this screen, then click **Finish** to dismiss the installer. |

## 13.1.3 Installing Oracle WebCenter Content on the Other Host Computers

If you have followed the EDG shared storage recommendations, there is a separate shared storage volume for product installations on WCCHOST2, and you must also install the software on WCCHOST2. For more information, see Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment.

## 13.1.4 Verifying the Installation

After you complete the installation, you can verify it by successfully completing the following tasks.

Reviewing the Installation Log Files

Checking the Directory Structure

Viewing the Contents of Your Oracle Home

### 13.1.4.1 Reviewing the Installation Log Files

Review the contents of the installation log files to make sure that no problems were encountered. For a description of the log files and where to find them, see "Understanding Installation Log Files" in *Installing Software with the Oracle Universal Installer*.

### 13.1.4.2 Checking the Directory Structure

The contents of your installation vary based on the options you selected during the installation.

The addition of Oracle WebCenter Content will add the following directory and sub-directories:

```
/u01/oracle/products/fmw/wccontent
common
plugins
ucm
wccadf

/u01/oracle/products/fmw/wccapture
capture
common
plugins
```

For more information about the directory structure you should see after installation, see "What are the Key Oracle Fusion Middleware Directories?" in *Understanding Oracle Fusion Middleware*.

#### 13.1.4.3 Viewing the Contents of Your Oracle Home

You can also view the contents of your Oracle home using the `viewInventory` script. For more information, see "Viewing the contents of an Oracle home" in *Installing Software with the Oracle Universal Installer*.

## 13.2 Creating the Oracle WebCenter Content Database Schemas

Before you can configure an Oracle WebCenter Content domain, you must install the required schemas in a certified database for use with this release of Oracle Fusion Middleware.

Follow the instructions in this section to install the schemas.

Starting the Repository Creation Utility (RCU)

Navigating the RCU Screens to Create the Schemas

### 13.2.1 Starting the Repository Creation Utility (RCU)

To start the Repository Creation Utility (RCU):

1. Navigate to the *ORACLE_HOME*`/oracle_common/bin` directory on your system.
2. Make sure the *JAVA_HOME* environment variable is set to the location of a certified JDK on your system. The location should be up to but not including the `bin` directory. For example, if your JDK is located in `/u01/oracle/products/jdk`:

   On UNIX operating systems:

   ```
   export JAVA_HOME=/u01/oracle/products/jdk
   ```

3. Start RCU:

   On UNIX operating systems:

   ```
   ./rcu
   ```

### 13.2.2 Navigating the RCU Screens to Create the Schemas

After you start the RCU, you can then use the wizard screens to select and install the required schemas for your Oracle Fusion Middleware product. Schema creation involves the following tasks.

**Task 1 Introducing RCU**
Click **Next**.

**Task 2 Selecting a Method of Schema Creation**
If you have the necessary permission and privileges to perform DBA activities on your database, select **System Load and Product Load**. This procedure assumes that you have the necessary privileges.

If you do not have the necessary permission or privileges to perform DBA activities in the database, you must select **Prepare Scripts for System Load** on this screen. This option will generate a SQL script, which can be provided to your database administrator. See "Understanding System Load and Product Load" in *Creating Schemas with the Repository Creation Utility*.

#### Task 3 Providing Database Connection Details

Provide the database connection details for RCU to connect to your database.

In the **Host Name** field, enter the SCAN address of the Oracle RAC Database.

Enter the **DBMS/Service** details.

Enter the **Schema Owner** and **Schema Password** details.

Click **Next** to proceed, then click **OK** on the dialog window confirming that connection to the database was successful.

#### Task 4 Specifying a Custom Prefix and Selecting Schemas

Select **existing prefix**, and select the prefix you created while configuring the initial domain.

From the list of schemas, expand the **WebCenter Content** schema section and select only the **Oracle WebCenter Content Server -- Complete** schema.

The custom prefix is used to logically group these schemas together for use in this domain only; you must create a unique set of schemas for each domain as schema sharing across domains is not supported.

> **Tip:**
> For more information about custom prefixes, see "Understanding Custom Prefixes" in *Creating Schemas with the Repository Creation Utility*.
>
> For more information about how to organize your schemas in a multi-domain environment, see "Planning Your Schema Creation" in *Creating Schemas with the Repository Creation Utility*.

> **Tip:**
> You must make a note of the custom prefix you choose to enter here; you will need this later on during the domain creation process.

Click **Next** to proceed, then click **OK** in the dialog window confirming that prerequisite checking for schema creation was successful.

#### Task 5 Specifying Schema Passwords

Specify how you want to set the schema passwords on your database, then specify and confirm your passwords.

> **Tip:**
> You must make a note of the passwords you set on this screen; you will need them later on during the domain creation process.

#### Task 6 Verifying the Tablespaces for the Required Schemas

On the Map Tablespaces screen, review the information, and then click **Next** to accept the default values.

Click **OK** in the confirmation dialog box.

**Task 7 Completing Schema Creation**

Navigate through the remainder of the RCU screens to complete schema creation. When you reach the Completion Summary screen, click **Close** to dismiss RCU.

**Task 8 Verifying the Schema Creation**

To verify that the schemas were created successfully, and to verify the database connection details, use SQL*Plus or another utility to connect to the database, using the OCS schema name and the password you provided.

For example:

```
./sqlplus

SQL*Plus: Release 11.2.0.4.0 Production on Fri Nov 1 08:44:18 2013

Copyright (c) 1982, 2013, Oracle.  All rights reserved.

Enter user-name: WCPEDG_OCS
Enter password: ocs_password

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL>
```

## 13.3 Extending the Domain for WebCenter Content

This section provides instructions for extending the existing enterprise deployment domain with the Oracle WebCenter Content software.

Extending the domain involves the following tasks.

Starting the Configuration Wizard

Navigating the Configuration Wizard Screens to Extend the Domain with WebCenter Content

### 13.3.1 Starting the Configuration Wizard

To start the Configuration Wizard:

1. Shut down the domain completely before extending the domain. From the WebLogic Server Console, stop all managed servers and verify, and then stop the Administration Server.
2. Navigate to the following directory and start the WebLogic Server Configuration Wizard.

   ```
   cd ORACLE_HOME/oracle_common/common/bin
   ./config.sh
   ```

### 13.3.2 Navigating the Configuration Wizard Screens to Extend the Domain with WebCenter Content

Follow the instructions in this section to extend the domain for the topology.

**Note:**

You can use the procedure described in this section to extend an existing domain. If your needs do not match the instructions given in the procedure, be sure to make your selections accordingly, or refer to the supporting documentation for additional details.

Domain extension and configuration includes the following tasks:

### Task 1 Selecting the Domain Type and Domain Home Location

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the ASERVER_HOME variable, which represents the complete path to the Administration domain home you created as part of the initial domain.

For more information about the directory location variables, see File System and Directory Variables Used in This Guide.

**Tip:**
More information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 2 Selecting the Configuration Template

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle Universal Content Management - Content Server - 12.2.1.1.0 [wccontent]**

  In addition, the following additional templates should already be selected, because they were used to create the initial Infrastructure domain:

  - **Oracle Enterprise Manager - 12.2.1.1.0 [em]**
  - **Oracle JRF - 12.2.1.1.0 [oracle_common]**
  - **WebLogic Coherence Cluster Extension - 12.2.1.1.0 [wlserver]**

  In addition, the following templates are also already selected, because they were used to extend the domain with WebCenter Portal:

  - **Oracle WebCenter Portal - 12.2.1.1.0 [wcportal]**
  - **Oracle WebCenter Pagelet Producer - 12.2.1.1.0 [wcportal]**
  - **Oracle WebCenter Portlet Producer - 12.2.1.1.0 [wcportal]**
  - **Oracle WebCenter Discussion Server - 12.2.1.1.0 [wcportal]**
  - **Oracle WebCenter Analytics Collector - 12.2.1.1.0 [wcportal]**

**Tip:**
More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 3 Specifying the Database Configuration Type**

On the Database Configuration Type screen, select **RCU Data**.

All fields are pre-populated, because you already configured the domain to reference the Fusion Middleware schemas that are required for the Infrastructure domain.

Verify and ensure that credentials in all the fields are the same that you have provided while configuring the Oracle Fusion Middleware Infrastructure.

Click **Get RCU Configuration** after you finish verifying the database connection information. The following output in the Connection Result Log indicates that the operating succeeded:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK

Successfully Done.
```

**Tip:**

For more information about the **RCU Data** option, see "Understanding the Service Table Schema" in *Creating Schemas with the Repository Creation Utility*.

For more information about the other options on this screen, see "Datasource Defaults" in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 4 Specifying JDBC Component Schema Information**

On the JDBC Component Schema screen, select all the UCM schemas (for WebCenter Content) in the table.

When you select the schemas, the fields on the page are activated and the database connection fields are populated automatically.

Click **Convert to GridLink** and click **Next**.

**Task 5 Providing the GridLink Oracle RAC Database Connection Details**

On the GridLink Oracle RAC Component Schema screen, provide the information required to connect to the RAC database and component schemas, as shown in the following table.

| Element | Description and Recommended Value |
|---|---|
| SCAN, Host Name, and Port | Select the **SCAN** check box.<br>In the **Host Name** field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database.<br>In the **Port** field, enter the SCAN listening port for the database (for example, `1521`) |
| ONS Host and Port | In the **ONS Host** field, enter the SCAN address for the Oracle RAC database.<br>In the **Port** field, enter the ONS Remote port (typically, `6200`). |
| Enable Fan | Verify that the **Enable Fan** check box is selected, so the database can receive and process FAN events. |

### Task 6 Testing the JDBC Connections

Use the JDBC Component Schema Test screen to test the data source connections you have just configured.

A green check mark in the **Status** column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

> **Tip:**
> For more information about the other options on this screen, see "Test Component Schema" in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 7 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

- **Topology**
- **File store**

### Task 8 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server for Oracle WebCenter Content appears in the list of servers.

Perform the following tasks to modify the default Oracle WebCenter Content Managed Server and create a second Managed Server:

1. Rename the default Managed Server to `WLS_WCC1`.
2. Click **Add** to create a new Managed Server and name it `WLS_WCC2`.

   > **Tip:**
   > The server names recommended here will be used throughout this document; if you choose different names, be sure to replace them as needed.

3. Use the information in the following table to fill in the rest of the columns for each Oracle WebCenter Content Managed Server.

| Server Name | Listen Address | Listen Port | Enable SSL | SSL Listen Port | Server Groups |
|---|---|---|---|---|---|
| WLS_WCC1 | WCCHOST1 | 16200 | Unchecked | Disabled | UCM-MGD-SVR |
| WLS_WCC2 | WCCHOST2 | 16200 | Unchecked | Disabled | UCM-MGD-SVR |

> **Tip:**
> More information about the options on the Managed Server screen can be found in Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 9 Configuring a Cluster**

In this task, you create a cluster of Managed Servers to which you can target the Oracle WebCenter Content software.

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify `WCC_Cluster` in the **Cluster Name** field.
3. Leave the **Cluster Address** field blank.

---

**Note:**
By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to "Considerations for Choosing Unicast or Multicast" in *Administering Clusters for Oracle WebLogic Server*.

---

**Tip:**
More information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 10 Assigning Managed Servers to the Cluster**

Use the Assign Servers to Clusters screen to assign `WLS_WCC1` and `WLS_WCC2` to the new cluster, `WCC_Cluster`:

1. In the Clusters pane, select the cluster to which you want to assign the servers; in this case, `WCC_Cluster`.
2. In the Servers pane, assign WLS_WCC1 to `WCC_Cluster` by doing one of the following:
   - Click once on the `WLS_WCC1` Managed Server to select it, then click on the right arrow to move it beneath the selected cluster in the Clusters pane.
   - Double-click on `WLS_WCC1` to move it beneath the selected cluster in the clusters pane.
3. Repeat to assign `WLS_WCC2` to `WCC_Cluster`.

**Tip:**
More information about the options on this screen can be found in Assign Servers to Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 11 Configuring Coherence Clusters**

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at **9991**, as it was defined during the initial Infrastructure domain creation.

**Note:**
For Coherence licensing information, refer to "Oracle Coherence" in *Oracle Fusion Middleware Licensing Information*.

**Task 12 Creating Machines for WebCenter Content Servers**
Use the Machines screen to add two new machines:

1. Click the **Add** button.
2. Enter WCCHOST1 in the **Name** field.
3. Enter the host name of WCCHOST1 for the Node Manage Listener address. Leave the Node Manager port to the default value of `5556`.
4. Repeat the above steps for WCCHOST2.

Under the **Unix Machine** tab, verify the names of the machines you created when creating the initial Infrastructure domain, as shown in the following table.

Click **Next** to proceed.

| Name | Node Manager Listen Address | Node Manager Listen Port |
|---|---|---|
| WCCHOST1 | The value of the WCCHOST1 host name variable. For example, `WCCHOST1.example.com`. | 5556 |
| WCCHOST2 | The value of the WCCHOST2 host name variable. For example, `WCCHOST2.example.com`. | 5556 |

**Task 13 Assigning Servers to Machines**
Use the Assign Servers to Machines screen to assign the Oracle WebCenter Content Managed Servers you just created to the corresponding machines in the domain.

Assign WLS_WCC1 to WCCHOST1, and assign WLS_WCC2 to WCCHOST2.

**Tip:**
More information about the options on this screen can be found in Assign Servers to Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 14 Creating Virtual Targets**
Click **Next** to proceed to the next screen.

**Task 15 Creating Partitions**
Click **Next** to proceed to the next screen.

**Task 16 Configuring the JMS File Store**
In the JMS File Stores screen, assign the following directory for each of the WebCenter Content Persistence stores including Content Server JMS file stores:

*ORACLE_RUNTIME/domain_name/WCC_Cluster/*jms

**Note:** Create the `jms` folder before starting the managed servers.

In this example, replace *RUNTIME_HOME* with the value of the variable for you environment. Replace *WCC_Cluster* with the name you assigned to the WebCenter Content cluster.

Select **Direct-Write** from the drop-down list for **Synchronous Write Policy** (for both the stores).

**Task 17 Reviewing Your Configuration Specifications and Configuring the Domain**

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain extension will not begin until you click **Update**.

**Tip:**
More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 18 Writing Down Your Domain Home and Administration Server URL**

The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server.

Click **Finish** to dismiss the configuration wizard.

**Task 19 Start the Administration Server**

Start the Administration Server to ensure the changes you have made to the domain have been applied.

## 13.4 Completing Postconfiguration and Verification Tasks for WebCenter Content

Several configuration and validation steps must be performed to bring the content servers online. Complete the following sections in the order listed.

Propagating the Extended Domain to the Domain Directories and Machines

Restarting and Validating Pre-existing Managed Servers

Modifying the Upload and Stage Directories to an Absolute Path
: After configuring the domain and unpacking it to the Managed Server domain directories on all the hosts, verify and update the `upload` and `stage` directories for the new Managed Servers.

Starting the Node Manager on WCCHOST1
: After you unpack the extended domain on WCCHOST1, you can start the Node Manager from the Managed Server directory on WCCHOST1.

Starting the WLS_WCC1 Managed Server

Configuring the Content Server on WLS_WCC1 Managed Server

Updating the cwallet File in the Administration Server

Starting the Node Manager on WCCHOST2
: After you have propagated the domain configuration to WCCHOST2, you can start the Node Manager for the *MSERVER_HOME* domain directory.

Starting the WLS_WCC2 Managed Server

Configuring the Content Server on WLS_WCC2 Managed Server

Validating GridLink Data Sources

Configuring Additional Parameters

Configuring Service Retries for Oracle WebCenter Content

Granting the WebCenter Content Administrative Roles via Credential Map

### 13.4.1 Propagating the Extended Domain to the Domain Directories and Machines

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 WCPHOST1 to create a template pack:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true
          -domain=ASERVER_HOME
          -template=/full_path/edgdomaintemplateWCC.jar
          -template_name=edgdomain_templateWCC
```

In this example:

- Replace *ASERVER_HOME* with the actual path to the domain directory you created on the shared storage device.
- Replace *full_path* with the complete path to the directory where you want the template jar file saved.
- `edgdomaintemplateWCC.jar` is a sample name for the JAR file you are creating, which will contain the domain configuration files, including the configuration files for the Oracle HTTP Server instances.

- `edgdomain_templateWCC` is the name assigned to the domain template file.

3. Run the following `unpack` command on WCPHOST1 to propagate the template created in the preceding step to the *MSERVER_HOME* directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME
            -template=/full_path/edgdomaintemplateWCC.jar
            -app_dir=APPLICATION_HOME
            -overwrite_domain=true
```

In this example:

- Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
- `edgdomaintemplateWCC.jar`is the directory path and name of the template you created when you ran the pack command to pack up the domain on the shared storage device.
- The `-overwrite_domain=true` argument is necessary when you are 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.
- Replace *`APPLICATION_HOME`* with the complete path to the Application directory for the domain on local storage.

  **Tip:**

  For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

4. Run the following command on WCPHOST1 to copy the template pack created in step 1 to WCPHOST2, WCCHOST1, and WCCHOST2:

```
scp /full_path/edgdomaintemplateWCC.jar oracle@WCPHOST2:/full_path/
scp /full_path/edgdomaintemplateWCC.jar oracle@WCCHOST1:/full_path/
scp /full_path/edgdomaintemplateWCC.jar oracle@WCCHOST2:/full_path/
```

5. Run the following `unpack` command on each of the remote hosts to deploy the domain template copied in the preceding step to the *MSERVER_HOME* directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME
            -template=/full_path/edgdomaintemplateWCC.jar
            -app_dir=APPLICATION_HOME
            -overwrite_domain=true
```

In this example:

- Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
- `edgdomaintemplateWCC.jar`is the directory path and name of the template you created when you ran the pack command to pack up the domain on the shared storage device.
- The `-overwrite_domain=true` argument is necessary when you are 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.
- Replace *`APPLICATION_HOME`* with the complete path to the Application directory for the domain on local storage.

  **Tip:**

  For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

## 13.4.2 Restarting and Validating Pre-existing Managed Servers

Restart the managed servers for the pre-existing components now that the domain has been extended and unpacked to the *MSERVER_HOME* directories on all of the servers.

1. From the WebLogic Server Console, restart the WLS_WSM*n* Managed Servers for the WebServices Manager Policy Manager.
2. From another browser window, verify the WSM-PM application is responding by successfully loading the URL:

   ```
   http://wcpinternal.example.com/wsm-pm/validator
   ```
3. From the WebLogic Server Console, restart the WC_Collaboration*n* and WC_Portlet*n* Managed Servers for the WebCenter Portal Services
4. From another browser window, verify the Discussions and Portlet applications are responding by successfully loading the URLs:

   ```
   https://wcp.example.com/owc_discussions
   http://wcpinternal.example.com/portalTools
   ```
5. From the WebLogic Server Console, restart the WC_Portal*n* Managed Servers for the WebCenter Portal.
6. From another browser window, verify the Discussions and Portlet application is responding by successfully loading the URL:

   ```
   https://wcp.example.com/webcenter
   ```

### 13.4.3 Modifying the Upload and Stage Directories to an Absolute Path

After configuring the domain and unpacking it to the Managed Server domain directories on all the hosts, verify and update the `upload` and `stage` directories for the new Managed Servers.

This step is necessary to avoid potential issues when performing remote deployments and for deployments that require the stage mode.

To update these directory paths for all the Managed Servers in the Managed Server domain home directory:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the left navigation tree, expand **Domain**, and then **Environment**.
3. Click **Lock & Edit**.
4. Click **Servers**.
5. For each new Managed Server in the Managed Server domain home directory:
   a. Click the name of the Managed Server.
   b. Click the **Configuration** tab, and then click the **Deployment** tab.
   c. Verify that the **Staging Directory Name** is set to the following:

      *MSERVER_HOME*/servers/*server_name*/stage

      Replace *MSERVER_HOME* with the directory path for the MSERVER_HOME directory; replace *server_name* with the name of the Server you are editing.

   d. Update the **Upload Directory Name** to the following value:

      *ASERVER_HOME*/servers/AdminServer/upload

      Replace *ASERVER_HOME* with the directory path for the ASERVER_HOME directory.

   e. Click **Save**.
   f. Return to the Summary of Servers screen.
6. When you have modified these values for each Managed Server, click **Activate Changes**.

### 13.4.4 Starting the Node Manager on WCCHOST1

After you unpack the extended domain on WCCHOST1, you can start the Node Manager from the Managed Server directory on WCCHOST1.

1. Navigate to the following directory on WCCHOST1:

   *MSERVER_HOME*/bin

2. Use the following command to start the Node Manager:

   ```
   nohup ./startNodeManager.sh > $MSERVER_HOME/nodemanager/nodemanager.out 2>&1 &
   ```

For information about additional Node Manager configuration options, see *Administering Node Manager for Oracle WebLogic Server*.

### 13.4.5 Starting the WLS_WCC1 Managed Server

To start the WLS_WCC1 Managed Server:

1. Log in to the Oracle WebLogic Server Administration Console at `http://admin.example.com/console`.
2. Start the WLS_WCC1 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_WCC1**, and then 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.

### 13.4.6 Configuring the Content Server on WLS_WCC1 Managed Server

To configure Content Server:

1. Log in to WLS_WCC1 at `http://WCCHOST1:16200/cs` using the `weblogic` user name and password to display a configuration page.

   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 *`RUNTIME_HOME`*`/WCDomain/WCC_Cluster`.
2. Change the following values on the server configuration page:

   Make sure that the **Is new Content Server Instance?** check box is selected.

   - **Content Server Instance Folder**: Set this to *`RUNTIME_HOME/domain_name/`*`WCC_Cluster/cs`.

     For example:`/u01/oracle/runtime/wcpedg_domain/WCC_Cluster/cs`
   - **Native File Repository Location**: Set this to *`RUNTIME_HOME/domain_name/`*`WCC_Cluster/cs/vault`.

     For example:`/u01/oracle/runtime/wcpedg_domain/WCC_Cluster/cs/vault`
   - **WebLayout Folder**: Set this to *`RUNTIME_HOME/domain_name/`*`WCC_Cluster/cs/weblayout`.

     For example:`/u01/oracle/runtime/wcpedg_domain/WCC_Cluster/cs/weblayout`

- **User Profile Folder**: Set this to *RUNTIME_HOME/domain_name/*`WCC_Cluster/cs/data/users/profiles`.

  For example:`/u01/oracle/runtime/wcpedg_domain/WCC_Cluster/cs/data/users/profiles`

- **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|
  wcpinternal.example.com-IP|load-balancer-IP
  ```

- **WebServer HTTP/HTTPS Address:** `wcp.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.
4. Restart the Managed Server by using the WebLogic Server Administration Console.

## 13.4.7 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.

When adding WebCenter Content to a WebCenter Portal enterprise deployment, you will have to copy the cwallet file from the WC Content host (WCCHOST1) to the WC Portal host (WCPHOST1) where the Administration Server is running.

To do this, copy the file to *ASERVER_HOME*`/config/fmwconfig` on WCPHOST1 using the following command (all on a single line):

```
scp -p \
WCCHOST1:/MSERVER_HOME/config/fmwconfig/cwallet.sso \
WCPHOST1:/ASERVER_HOME/config/fmwconfig/cwallet.sso
```

**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 WCPHOST1 at *ASERVER_HOME*`/config/fmwconfig`.

## 13.4.8 Starting the Node Manager on WCCHOST2

After you have propagated the domain configuration to WCCHOST2, you can start the Node Manager for the *MSERVER_HOME* domain directory.

1. If you haven't already, log in to WCCHOST2.

2. Change directory to the following location:

   *MSERVER_HOME*/bin

3. Use the following command to start the Node Manager on WCCHOST2:

   ```
   nohup ./startNodeManager.sh > $MSERVER_HOME/nodemanager/nodemanager.out 2>&1 &
   ```

   For more information about additional Node Manager configuration options, see *Administering Node Manager for Oracle WebLogic Server*.

### 13.4.9 Starting the WLS_WCC2 Managed Server

To start the WLS_WCC2 Managed Server:

1. Start the WLS_WCC2 Managed Server using the WebLogic Server Administration Console, as follows:

   a. Expand the **Environment** node in the **Domain Structure** 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.

### 13.4.10 Configuring the Content Server on WLS_WCC2 Managed Server

To configure Content Server:

1. Log in to WLS_WCC2 at `http://WCCHOST2:16200/cs` using the `weblogic` administration user name and password to display a configuration page.

   The Oracle WebCenter Content configuration files are on a shared disk so that all members of the cluster can access them. The shared disk location of the Oracle WebCenter Content enterprise deployment is at *ORACLE_RUNTIME*/WCDomain/WCC_Cluster.

2. Change the following values on the server configuration page:

   - **Content Server Instance Folder**: Set this to *ORACLE_RUNTIME*/WCDomain/WCC_Cluster/cs.
   - **Native File Repository Location**: Set this to *ORACLE_RUNTIME*/WCDomain/WCC_Cluster/cs/vault.
   - **WebLayout Folder**: Set this to *ORACLE_RUNTIME*/WCDomain/WCC_Cluster/cs/weblayout.
   - **User Profile Folder**: Set this to *ORACLE_RUNTIME*/WCDomain/WCC_Cluster/cs/data/users/profiles.
   - **Content Server URL Prefix**: `/cs/ (default value)`

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

3. Click **Submit** when finished.
4. Restart the Managed Server by using the WebLogic Server Administration Console.

## 13.4.11 Validating GridLink Data Sources

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.

Verifying the Configuration of a GridLink Data Source for WebCenter Content

Verifying the Configuration of ONS for a GridLink Data Source

### 13.4.11.1 Verifying the Configuration of a GridLink Data Source for WebCenter Content

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, select one of the servers, and click **Test Data Source**.

   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.

### 13.4.11.2 Verifying the Configuration of ONS for a 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.
6. In the **ONS** tab, select the **Testing** tab.
7. Select a server, and click **Test ONS**.

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

```
[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
```

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

## 13.4.12 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 for WCCHOST1 and WLS_WCC2 is for 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 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.

## 13.4.13 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 the non-LDAP WebLogic Server administration user name (for example, *weblogic*) 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**.

   These changes will take effect after a restart of all WebCenter Content Managed Servers, at the end of the procedure described in Granting the WebCenter Content Administrative Roles via Credential Map section.

---

**Note:**

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

*`ORACLE_RUNTIME/domain_name/cluster_name`*`/cs/config/config.cfg`

(You can also edit this file directly in a text editor. Remember to restart all WebCenter Content Managed Servers.

---

## 13.4.14 Granting the WebCenter Content Administrative Roles via Credential Map

You must configure the Credential map to grant the Content Server administrative roles to the **`WCPAdministrators`** LDAP group.

The **`WCPAdministrators`** LDAP group is created in the Provisioning an Enterprise Deployment Administration User and Group section completed earlier. This configuration of credential map ensures consistent use of the LDAP administrative user for all configuration, administration, and maintenance tasks.

To configure a credential map and provide the necessary role grants to the LDAP-based **`WCPAdministrators`** group:

1. Log in to content server using the *weblogic* account.
2. Expand the **Administration** menu, select **Credential Maps**.
3. In the Map Identifier Field, enter a name for the new credential map: **LDAPAdmins**.
4. Add the following lines to map the LDAP group to the multiple administrative roles:

```
# Assign full set of administration roles to the LDAP WCPAdministrators group
     WCPAdministrators, admin
     WCPAdministrators, sysmanager
     WCPAdministrators, refineryadmin
     WCPAdministrators, rmaadmin
     WCPAdministrators, pcmadmin
     WCPAdministrators, ermadmin
     #
     # Comment the following if you are not implementing Accounts in Content
Server.
     WCPAdministrators, @#all(RWDA)
     WCPAdministrators, @#none(RWDA)
```

**Note:** If you are not implementing **Accounts** in Content Server, comment the last two lines in the example above.

5. Click **Update**.
6. Navigate to **Administration** > **Providers**.
7. Click the **info** link for the existing JPS provider.
8. Make sure that the **Credential Map** parameter does not already have a map identifier listed.
9. Click the **Edit** button.
10. Enter the name of the Map Identifier from step 3 above as the Credential Map value.
11. Click **Update**.
12. Repeat step 6 through 11 for each WebCenter content instance.
13. Restart the managed servers in the **WCC_Cluster**.
14. Log in to each content server using the `weblogic_wcp` LDAP user and verify that the administrative menu options appear in the user interface.

## 13.5 Configuring Oracle HTTP Server for the WebCenter Content Cluster

The following sections provide instructions for configuring Oracle HTTP Server for the WebCenter Content Cluster.



### 13.5.1 Configuring Oracle HTTP Server for the WLS_WCC Managed Servers

To configure the Oracle HTTP Server instances in the web tier so they route requests correctly to the Oracle WebCenter Content cluster, use the following procedure to create an additional Oracle HTTP Server configuration file that creates and defines the parameters of the `wcp.example.com` virtual server. To configure Oracle HTTP Server for the WLS_WCC Managed Servers:

1. Log in to WEBHOST1 and change directory to the configuration directory for the first Oracle HTTP Server instance (`ohs1`).

   ```
   cd OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf/
   ```

   **Note:**

   There are separate directories for configuration and runtime instance files. The runtime files under the `.../OHS/instances/ohsn/*` folder should not be edited directly. Edit only the `.../OHS/ohsn/*` configuration files.

2. In the `wcp_vh.conf` file, add the following lines between the `<VirtualHost>` and `</VirtualHost>` tags:

```
#UCM
<Location /cs>
   WebLogicCluster WCCHOST1:16200,WCCHOST2:16200
   WLSRequest ON
   WLCookieName JSESSIONID
   WLProxySSL ON
   WLProxySSLPassThrough ON
</Location>

<Location /adfAuthentication>
   WebLogicCluster WCCHOST1:16200,WCCHOST2:16200
   WLSRequest ON
   WLCookieName JSESSIONID
   WLProxySSL ON
   WLProxySSLPassThrough ON
</Location>

<Location /_ocsh>
   WebLogicCluster WCCHOST1:16200,WCCHOST2:16200
   WLSRequest ON
   WLCookieName JSESSIONID
   WLProxySSL ON
   WLProxySSLPassThrough ON
</Location>
```

3. Copy the `wcp_vh.conf` file to the configuration directory for the second Oracle HTTP Server instance (`ohs2`):

   *OHS_DOMAIN_HOME*`/config/fmwconfig/components/`**`ohs2`**`/moduleconf/`

4. Edit the `wcp_vh.conf` and change any references of WEBHOST1 to WEBHOST2 in the `<VirtualHost>` directives.

5. Restart the Oracle HTTP server instances on WEBHOST1 and WEBHOST2.

## 13.5.2 Configuring the WebLogic Proxy Plug-In

Before you can validate that requests are routed correctly through the Oracle HTTP Server instances, you must set the `WebLogic Plug-In Enabled` parameter for the clusters you just configured.

1. Log in to the Oracle WebLogic Server Administration Console.

2. In the **Domain Structure** pane, expand the **Environment** node.

3. Click **Clusters**.

4. Select the cluster to which you want to proxy requests from Oracle HTTP Server.

   The **Configuration: General** tab is displayed.

5. Scroll down to the **Advanced** section and expand it.

6. Click **Lock & Edit** in the Change Center.

7. Set **WebLogic Plug-In Enabled** to **yes**.

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

9. Click **Activate Changes** in the Change Center.
10. Restart all Managed Servers in all of the clusters that you modified in this chapter.

### 13.5.3 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.

Verifying the URLs

Verifying the Cluster Nodes

#### 13.5.3.1 Verifying the URLs

To verify the URLs:

1. While WLS_WCC2 is running, stop WLS_WCC1 using the WebLogic Server Administration Console.
2. Access `https://wcp.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 `https://wcp.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.

#### 13.5.3.2 Verifying the Cluster Nodes

To verify the cluster node:

1. Log in to the following WebCenter Content page, using your administrator user and password credentials:

   ```
   https://wcp.example.com/cs/idcplg?IdcService=CONFIG_INFO
   ```

2. Browse to the Administration/Configuration for WCC_Cluster 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.

## 13.6 Configuring Oracle WebCenter Content for WebCenter Portal

This section describes tasks required for configuring Oracle WebCenter Content Server for use with WebCenter Portal.

This section includes the following topics.

Enabling Mandatory Content Server Components

Enabling and Configuring the Dynamic Converter Component

Configuring Additional Content Server Features

### 13.6.1 Enabling Mandatory Content Server Components

For WebCenter Portal, you must enable the following Content Server components:

- **WebCenterConfigure** - Enable it to configure an instance of Content Server for WebCenter Portal and Portal Framework applications.
- **Folders_g or FrameworkFolders** - Enable either of these components to specify the folder service configured on Content Server.
  - **Folders_g** - Provides a hierarchical folder interface to content in Content Server. For an Oracle WebCenter Portal instance patched from an earlier release that used the Folders_g component, you can continue to use Folders_g or choose to migrate to the FrameworkFolders interface. Oracle recommends that you migrate to the FrameworkFolders interface for better performance and so that you can use any new Content Server features.
  - **FrameworkFolders** - Provides a hierarchical folder interface similar to a conventional file system, for organizing and locating some or all of the content in the repository. FrameworkFolders is a scalable, enterprise solution and is intended to replace Folders_g as the folder service for Content Server. For new installations of Oracle WebCenter Portal, it is recommended that you enable the FrameworkFolders component on Content Server.

> **Note:** Make sure you enable AutoSuggestConfig component before you enable FrameworkFolders component.

For detailed steps, see Enabling Mandatory Components in *Administering Oracle WebCenter Portal*.

> **Note:**
>
> If Oracle WebCenter Portal is configured to use the Folders_g component, and Folders_g is not enabled, the following exception displays:
>
> ```
> SEVERE: UCM feature folders is not installed on server. at
> oracle.webcenter.content.integration.spi.ucm.UCMBridge.getBridge(UCMBridge.ja
> va:349) ....
> ```
>
> If Oracle WebCenter Portal is configured to use the FrameworkFolders component, and FrameworkFolders is not enabled, the following message is displayed:
>
> ```
> Foldering service from content server Folders_g and Portal Server
> Configuration FrameworkFolders do not match
> ```

### 13.6.2 Enabling and Configuring the Dynamic Converter Component

This task is optional, but strongly recommended.

This configuration is required for the Slide Previewer capability in WebCenter Portal, which makes use of the HTML renditions generated on the fly by the Dynamic Converter.

The configuration for the Dynamic Converter consists of two steps: enabling the Dynamic Converter, and defining the file types for which the Dynamic Converter is available. For detailed steps, see the Configuring the Dynamic Converter Component section in *Administering Oracle WebCenter Portal*.

### 13.6.3 Configuring Additional Content Server Features

There are several other Content Server features that, while not mandatory, can provide additional functionality in your WebCenter Portal enterprise deployment. For example, you can enable features such as Site Studio, OracleTextSearch, and so on.

To find out more, and for detailed steps, see the Configuration Roadmap for Content Server section in *Administering Oracle WebCenter Portal*.

## 13.7 Registering Oracle WebCenter Content with the WebCenter Portal Application

Perform the following steps to register Oracle WebCenter Content Server with the WebCenter Portal application.

---

**Note:**

For more information about Content Server registration, see the Configuring Back-end Data Repositories for Tools and Services section in *Oracle Fusion Middleware Administrator's Guide for Oracle WebCenter Portal*.

---

1. Log in to Enterprise Manager Fusion Middleware Control and navigate to the home page for your application.

   For example, to navigate to the home page for WebCenter Portal, expand **WebCenter** > **Portal** > **Server** > **WebCenter Portal (WC_Portal1)**.

   ---

   **Note:** Multiple **WebCenter Portal** entries will appear, one for each WebLogic Managed Server. Choose any one. The application registration in this section will apply to the entire portal.

   ---

2. From the **WebCenter Portal** menu, select **Settings**, and then **Service Configuration**.

3. From the list of services on the WebCenter Service Configuration page, select **Content Repository**.

4. To connect to a new content repository, click **Add**.

5. Enter a unique name for this connection, specify the content repository type, and indicate whether this connection is the active (or default) connection for the application.

   - **Connection Name**

     Enter a unique name for this content repository connection. The name must be unique (across all connection types) within the WebCenter Portal application.

   - **Repository Type**

Select the type of repository to which you want to connect: **Oracle Content Server**.

- **Active Connection**

  Make this the default content repository for your WebCenter Portal application.

  You can connect your WebCenter Portal application to multiple content repositories; all connections are used. One connection must be designated the default (or active) connection.

6. Enter additional content repository details for WebCenter Portal:

   - **Content Administrator**

     Enter a user name with administrative rights for this Content Server instance. This user is used to create and maintain folders for WebCenter Portal content and manage content access rights. Enter `sysadmin`. Configure a valid administrative user here. Administrative privileges are required for this connection so that operations can be performed on behalf of WebCenter Portal users.

   - **Portal Server Identifier**

     Enter the root folder under which all WebCenter Portal content is stored. Specify a content repository folder that does not yet exist and use the format: `/foldername`. For example: `/MyWebCenterPortal`. The Root Folder cannot be `/`, the root itself, and it must be unique across applications. The folder specified is created for you when the application starts up. Invalid entries include: `/`, `/foldername/`, `/foldername/subfolder`.

   - **Security Group**

     Enter a unique name for this WebCenter Portal application within this content repository. For example: **MyWCPApp**

     The name must begin with an alphabetical character, followed by any combination of alphanumeric characters or the underscore character. The string must be less than or equal to fourteen characters.

     This name is used to separate data when multiple WebCenter Portal applications share the same content repository and should be unique across applications. It is also used to name document-related workflows, the security group in which all data created in that Portals application is stored, security roles, as well as to stripe user permissions and default attributes for a particular WebCenter Portal instance.

7. Enter connection details for the content repository:

   - **RIDC Socket Type**

     Select **Socket** - Use an intradoc socket connection to connect to Content Server.

     The client IP address must be added to the list of authorized addresses in the Content Server. In this case, the client is the machine on which Oracle WebCenter Portal is running.

   - **Server Host**

     Enter the Load Balancer address, **wcpinternal.example.com**, so that requests to `/cs` use any available Content Server node.

The IP address for the virtual host configured on the load balancer and the Self-IP of the load balancer must be added to the Content Server's Incoming Socket Connection Address Security Filter.

---

**Note:**

If you have not done so already, add a rule to your Load Balancer that specifies how to route WebCenter Content traffic, for example:

```
(LBR)10.110.10.135:6300 -> 10.110.10.23:4444 (WCCHOST1) & 10.110.10.24:4444
(WCCHOST2)
```

---

- **Server Port**

  Enter the port on which the Content Server listens: **6300**

- **Connection Timeout (ms)**

  Specify the length of time allowed to log in to Content Server (in milliseconds) before issuing a connection timeout message. If no timeout is set, there is no time limit for the login operation. Select a reasonable timeout depending on your environment. For example: **60000**.

- **Authentication Method**

  Select **Identity Propagation** - In this enterprise deployment, Content Server and the WebCenter Portal application both use the same identity store to authenticate users.

- **Web Context Root**

  Enter **/cs** as the Web server context root for Content Server.

- **Administrator User Name**

  Enter a user name with administrative rights for this Oracle Content Server instance. This user will be used to fetch content type information based on profiles and track document changes for WebCenter Portal cache invalidation. Defaults to `sysadmin`.

- **Administrator Password**

  Leave Empty. An Administrator Password value is only required when the `socketType` is set to `web`.

8. Click **OK** to save this connection.
9. To start using the new (active) connection you must restart the Managed Server on which the WebCenter Portal application is deployed.

# 14

# Extending the Domain to Include Inbound Refinery

The following topics describe how to extend the enterprise deployment domain to include Inbound Refinery software.

Extending the Domain for Inbound Refinery
: This section provides instructions for extending the existing enterprise deployment domain with the Inbound Refinery software.

Completing Postconfiguration and Verification Tasks for Inbound Refinery
: This section describes how to do post-configuration and verification tasks for Inbound Refinery.

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.

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.

## 14.1 Extending the Domain for Inbound Refinery

This section provides instructions for extending the existing enterprise deployment domain with the Inbound Refinery software.

Starting the Configuration Wizard

Navigating the Configuration Wizard Screens to Extend the Domain

### 14.1.1 Starting the Configuration Wizard

To start the Configuration Wizard:

1. Shut down the domain completely before extending the domain. From the WebLogic Server Console, stop all managed servers and verify, and then stop the Administration Server.
2. Navigate to the following directory and start the WebLogic Server Configuration Wizard.

```
cd ORACLE_HOME/oracle_common/common/bin
./config.sh
```

### 14.1.2 Navigating the Configuration Wizard Screens to Extend the Domain

Follow the instructions in this section to update and configure the domain for the topology.

---

**Note:**

You can use the same procedure described in this section to extend an existing domain. If your needs do not match the instructions given in the procedure, be sure to make your selections accordingly, or refer to the supporting documentation for additional details.

---

Domain creation and configuration includes the following tasks:

**Task 1 Selecting the Domain Type and Domain Home Location**

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the *ASERVER_HOME* variable, which represents the complete path to the initial Administration Server domain home you created.

For more information about the directory location variables, see File System and Directory Variables Used in This Guide.

**Tip:**
More information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 2 Selecting the Configuration Template**

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle Universal Content Management - Inbound Refinery - 12.2.1.1.0 [wccontent]**

  The Infrastructure templates, WebCenter Portal templates, and WebCenter Content templates should already be selected, because they were used to create and update the initial domain.

  **Tip:**
  More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 3 Providing the GridLink Oracle RAC Database Connection Details**

On the GridLink Oracle RAC Component Schema screen, click **Next**.

**Task 4 Testing the JDBC Connections**

Click **Next** to continue.

**Task 5 Selecting Advanced Configuration**
To complete domain configuration for the topology, select the following option on the Advanced Configuration screen:

- **Topology**

**Task 6 Configuring Managed Servers**
On the Managed Servers screen, a new Managed Server appears in the list of servers.

Perform the following tasks to modify the default Managed Server and create a second Managed Server:

1. Rename the default Managed Server to `WLS_IBR1`.
2. Click **Add** to create a new Managed Server and name it `WLS_IBR2`.

   **Tip:**

   The server names recommended here will be used throughout this document. If you choose different names be sure to replace them as needed.

3. Use the information in the following table to fill in the rest of the columns for each Managed Server.

| Server Name | Listen Address | Listen Port | Enable SSL | SSL Listen Port | Server Group |
|---|---|---|---|---|---|
| WLS_IBR1 | WCCHOST1 | 16250 | No | Disabled | IBR-MGD-SVR |
| WLS_IBR2 | WCCHOST2 | 16250 | No | Disabled | IBR-MGD-SVR |

**Tip:**
More information about the options on the Managed Server screen can be found in Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 7 Configuring a Cluster**
In this task, you create a cluster of Managed Servers to which you can target the Oracle Inbound Refinery software.

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify `IBR_Servers` in the **Cluster Name** field.

**Note:**
By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to "Considerations for Choosing Unicast or Multicast" in *Administering Clusters for Oracle WebLogic Server*.

**Tip:**
More information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 8 Assigning Managed Servers to the Cluster

Use the Assign Servers to Clusters screen to assign `WLS_IBR1` and `WLS_IBR2` to the new cluster `IBR_Servers`:

1. In the Clusters pane, select the cluster to which you want to assign the servers; in this case, `IBR_Servers`.
2. In the Servers pane, assign WLS_IBR1 to `IBR_Servers` by doing one of the following:
   - Click once on `WLS_IBR1` Managed Server to select it, then click on the right arrow to move it beneath the selected cluster in the Clusters pane.
   - Double-click `WLS_IBR1` to move it beneath the selected cluster in the clusters pane.
3. Repeat to assign `WLS_IBR2` to `IBR_Servers`.

**Tip:**
More information about the options on this screen can be found in Assign Servers to Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 9 Configuring Coherence Clusters

Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at `9991`, as it was defined during the initial Infrastructure domain creation.

**Note:**
For Coherence licensing information, refer to "Oracle Coherence" in *Oracle Fusion Middleware Licensing Information*.

### Task 10 Verifying the Existing Machines

Under the **Unix Machine** tab, verify the names of the machines you created when creating the initial Infrastructure domain.

Click **Next** to proceed.

### Task 11 Assigning Servers to Machines

Use the Assign Servers to Machines screen to assign the Oracle Inbound Refinery Managed Servers you just created to the corresponding machines in the domain.

Assign `WLS_IBR1` to WCCHOST1, and assign `WLS_IBR2` to WCCHOST2.

**Tip:**
More information about the options on this screen can be found in Assign Servers to Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 12 Creating Virtual Targets**
Click **Next** to proceed to the next screen.

**Task 13 Creating Partitions**
Click **Next** to proceed to the next screen.

**Task 14 Reviewing Your Configuration Specifications and Configuring the Domain**
The Configuration Summary screen contains the detailed configuration information for the domain. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation will not begin until you click **Update**.

**Tip:**
More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 15 Writing Down Your Domain Home and Administration Server URL**
The Configuration Success screen will show the following items about the domain you just configured:

- Domain Location
- Administration Server URL

You must make a note of both items as you will need them later; the domain location is needed to access the scripts used to start the Node Manager and Administration Server, and the URL is needed to access the Administration Server.

Click **Finish** to dismiss the Configuration Wizard.

**Task 16 Start the Administration Server**
Start the Administration Server to ensure the changes you have made to the domain have been applied.

## 14.2 Completing Postconfiguration and Verification Tasks for Inbound Refinery

This section describes how to do post-configuration and verification tasks for Inbound Refinery.

Propagate the Domain Configuration Updates for Inbound Refinery

Modifying the Upload and Stage Directories to an Absolute Path
: After configuring the domain and unpacking it to the Managed Server domain directories on all the hosts, verify and update the `upload` and `stage` directories for the new Managed Servers.

Starting the Inbound Refinery Managed Servers

## 14.2.1 Propagate the Domain Configuration Updates for Inbound Refinery

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 backup copy of the Managed Server domain directory and the Managed Server `applications` directory.
2. Run the following `pack` command on WCPHOST1 to create a template pack:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true
          -domain=ASERVER_HOME
          -template=/full_path/edgdomaintemplateIBR.jar
          -template_name=edgdomain_templateIBR
```

   In this example:

   - Replace *ASERVER_HOME* with the actual path to the domain directory you created on the shared storage device.
   - Replace *full_path* with the complete path to the directory where you want the template jar file saved.
   - `edgdomaintemplateIBR.jar` is a sample name for the JAR file you are creating, which will contain the domain configuration files, including the configuration files for the Oracle HTTP Server instances.
   - `edgdomain_templateIBR` is the name assigned to the domain template file.

3. Run the following `unpack` command on WCPHOST1 to propagate the template created in the preceding step to the *MSERVER_HOME* directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME
            -template=/full_path/edgdomaintemplateIBR.jar
            -app_dir=APPLICATION_HOME
            -overwrite_domain=true
```

   In this example:

   - Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
   - `edgdomaintemplateIBR.jar`is the directory path and name of the template you created when you ran the pack command to pack up the domain on the shared storage device.

- The `-overwrite_domain=true` argument is necessary when you are 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.

- Replace *`APPLICATION_HOME`* with the complete path to the Application directory for the domain on local storage.

  **Tip:**

  For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

4. Run the following command on WCPHOST1 to copy the template pack created in step 1 to WCPHOST2, WCCHOST1, and WCCHOST2:

   ```
   scp /full_path/edgdomaintemplateIBR.jar oracle@WCPHOST2:/full_path/
   scp /full_path/edgdomaintemplateIBR.jar oracle@WCCHOST1:/full_path/
   scp /full_path/edgdomaintemplateIBR.jar oracle@WCCHOST2:/full_path/
   ```

   Replace *full_path* with the complete path to the directory where you want to copy the template jar file.

5. Run the following `unpack` command on each of the remote hosts to deploy the domain template copied in the preceding step to the *MSERVER_HOME* directory:

   ```
   cd ORACLE_COMMON_HOME/common/bin

   ./unpack.sh -domain=MSERVER_HOME
               -template=/full_path/edgdomaintemplateIBR.jar
               -app_dir=APPLICATION_HOME
               -overwrite_domain=true
   ```

   In this example:

   - Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.

   - `edgdomaintemplateIBR.jar`is the directory path and name of the template you created when you ran the pack command to pack up the domain on the shared storage device.

   - The `-overwrite_domain=true` argument is necessary when you are 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.

   - Replace *`APPLICATION_HOME`* with the complete path to the Application directory for the domain on local storage.

**Tip:**

For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

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. Log in to the Administration Console using the credentials for the `weblogic` user.
7. Restart the WLS_WSM*n*, WC_Collaboration*n*, WC_Portlet*n*, WLS_WCC*n*, and WC_Portal*n* managed servers.

## 14.2.2 Modifying the Upload and Stage Directories to an Absolute Path

After configuring the domain and unpacking it to the Managed Server domain directories on all the hosts, verify and update the `upload` and `stage` directories for the new Managed Servers.

This step is necessary to avoid potential issues when performing remote deployments and for deployments that require the stage mode.

To update these directory paths for all the Managed Servers in the Managed Server domain home directory:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the left navigation tree, expand **Domain**, and then **Environment**.
3. Click **Lock & Edit**.
4. Click **Servers**.
5. For each new Managed Server in the Managed Server domain home directory:
   a. Click the name of the Managed Server.
   b. Click the **Configuration** tab, and then click the **Deployment** tab.
   c. Verify that the **Staging Directory Name** is set to the following:

      ```
      MSERVER_HOME/servers/server_name/stage
      ```

      Replace *`MSERVER_HOME`* with the directory path for the MSERVER_HOME directory; replace *server_name* with the name of the Server you are editing.
   d. Update the **Upload Directory Name** to the following value:

      ```
      ASERVER_HOME/servers/AdminServer/upload
      ```

      Replace *`ASERVER_HOME`* with the directory path for the ASERVER_HOME directory.
   e. Click **Save**.
   f. Return to the Summary of Servers screen.
6. When you have modified these values for each Managed Server, click **Activate Changes**.

### 14.2.3 Starting the Inbound Refinery Managed Servers

To start the `WLS_IBR1` Managed Server on WCCHOST1:

1. Log in to the Oracle WebLogic Server Administration Console as the `weblogic_wcp` user at:

   `http://admin.example.com/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.

4. Repeat the preceding steps to start the `WLS_IBR2` Managed Server on WCCHOST2.

## 14.3 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 post-installation steps with Inbound Refinery.

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

Configuring Inbound Refinery Settings
: After you start the Inbound Refinery Managed Servers, configure the settings for each server on its post-installation configuration screen.

Granting the Inbound Refinery Administrative Roles via Credential Map

Specifying the Font Path

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.

## 14.3.1 Configuring Inbound Refinery Settings

After you start the Inbound Refinery Managed Servers, configure the settings for each server on its post-installation configuration screen.

To configure the settings for each Inbound Refinery instance:

1. Create the runtime cluster subdirectories required for the Oracle WebCenter Content Inbound Refinery shared folder configuration.

   The Oracle WebCenter Content Inbound Refinery 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 Inbound Refinery enterprise deployment is located at *RUNTIME_HOME*/*domain_name*/IBR_Servers/.

   Run the following commands to create the required subdirectories for every IBR managed server:

   ```
   mkdir -p RUNTIME_HOME/domain_name/IBR_Servers/ibr1/vault
   mkdir -p RUNTIME_HOME/domain_name/IBR_Servers/ibr1/weblayout
   mkdir -p RUNTIME_HOME/domain_name/IBR_Servers/ibr1/data/users/profiles
   mkdir -p RUNTIME_HOME/domain_name/IBR_Servers/ibr2/vault
   mkdir -p RUNTIME_HOME/domain_name/IBR_Servers/ibr2/weblayout
   mkdir -p RUNTIME_HOME/domain_name/IBR_Servers/ibr2/data/users/profiles
   ```

2. Access the Inbound Refinery post-installation configuration screen at the following URL, in which *N* is 1 or 2:

   ```
   http://WCCHOSTN:16250/ibr/
   ```

3. On the Configuration screen, you will see **Inbound Refinery Instance Identifier:** *name*. Set the configuration settings for this instance as follows. Each Inbound Refinery instance is independent of the other instances and local to each machine. Use local directories for the configuration directories of each instance.

   - **Inbound Refinery Instance Folder**: Set this to *RUNTIME_HOME*/*domain_name*/IBR_Servers/ibr*N*.

     For example: /u01/oracle/runtime/wcpedg_domain/IBR_Servers/ibr1

   - **Native File Repository Location**: Set this to *RUNTIME_HOME*/*domain_name*/IBR_Servers/ibr*N*/vault.

     For example: /u01/oracle/runtime/wcpedg_domain/IBR_Servers/ibr1/vault

   - **WebLayout Folder**: Set this to *RUNTIME_HOME*/*domain_name*/IBR_Servers/ibr*N*/weblayout.

     For example: /u01/oracle/runtime/wcpedg_domain/IBR_Servers/ibr1/weblayout

   - **User Profile Folders**: Set this to *RUNTIME_HOME*/*domain_name*/IBR_Servers/ibr*N*/data/users/profiles.

For example: `/u01/oracle/runtime/wcpedg_domain/IBR_Servers/ibr1/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|WEBHOST1-IP|WEBHOST2-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/runtime/wcpedg_domain/IBR_Servers/ibr`*N*`/config/config.cfg` file and then restarting the Inbound Refinery Managed Server.

  Where *N* is 1 for `http://WCCHOST1:16250/ibr/` and *N* is 2 for `http://WCCHOST2:16250/ibr/`

- **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 `/u01/oracle/runtime/wcpedg_domain/IBR_Servers/ibr`*N*`/config/config.cfg`.

  Where *N* is 1 for `http://WCCHOST1:16250/ibr/` and *N* is 2 for `http://WCCHOST2:16250/ibr/`

- **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.
```

4. Restart the Inbound Refinery Managed Server, using the WebLogic Server Administration Console.
5. Repeat the preceding steps for each Inbound Refinery instance, using different names for the content folders.

## 14.3.2 Granting the Inbound Refinery Administrative Roles via Credential Map

You must configure the Credential map to grant the Inbound Refinery administrative roles to the **`WCPAdministrators`** LDAP group.

The **`WCPAdministrators`** LDAP group is created in the Provisioning an Enterprise Deployment Administration User and Group section completed earlier. This configuration of credential map ensures consistent use of the LDAP administrative user for all configuration, administration, and maintenance tasks.

To configure a credential map and provide the necessary role grants to the LDAP-based **`WCPAdministrators`** group:

1. Log in to Inbound Refinery server on WCCHOST1 using the *weblogic* account.
2. Expand the **Administration** menu, select **Credential Maps**.
3. In the Map Identifier Field, enter a name for the new credential map: **LDAPAdmins**.
4. Add the following lines to map the LDAP group to the multiple administrative roles:

```
# Assign full set of administration roles to the LDAP WCPAdministrators group
     WCPAdministrators, admin
     WCPAdministrators, sysmanager
     WCPAdministrators, refineryadmin
     WCPAdministrators, rmaadmin
     WCPAdministrators, pcmadmin
     WCPAdministrators, ermadmin
     #
     # Comment the following if you are not implementing Accounts in Content
Server
     WCPAdministrators, @#all(RWDA)
     WCPAdministrators, @#none(RWDA)
```

   **Note:** If you are not implementing **Accounts** in Content Server, comment the last two lines in the example above.

5. Click **Update**.
6. Navigate to **Administration** > **Providers**.
7. Click the **info** link for the existing JPS provider.
8. Make sure that the **Credential Map** parameter does not already have a map identifier listed.
9. Click the **Edit** button.
10. Enter the name of the Map Identifier from step 3 above as the Credential Map value.
11. Click **Update**.
12. Repeat step 6 through 11 for each inbound refinery instance.
13. Restart the managed servers in the **IBR_Servers** cluster.
14. Log in to each Inbound Refinery server using the `weblogic_wcp` LDAP user and verify that the administrative menu options appear in the user interface.

## 14.3.3 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*.

## 14.3.4 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.

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.

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.

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.

### 14.3.4.1 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 Configuring Inbound Refinery Settings; for example, 5555. This is the `IntradocServerPort` value in the Inbound Refinery`config.cfg` file.
- **Instance Name:** The server instance name for Inbound Refinery as specified in 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.

9. Complete steps 1 through 8 for the second IBR server.

For more information about setting up providers, see "Configuring Content Server and Refinery Communication" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

#### 14.3.4.2 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:

   ```
   https://wcp.example.com/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 both Content Servers by restarting the WebCenter Content Managed Servers, using the WebLogic Server Administration Console.

#### 14.3.4.3 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:

   `https://wcp.example.com/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 the wizard does not list. For more information, see "Managing File Types" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

## 14.4 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 Conten*t.

For information about the conversion process, see "Configuring Content Servers to Send Jobs to Refineries" in *Oracle Fusion Middleware Managing Oracle WebCenter Content*.

# 15

# Extending the Domain with Oracle SOA Suite

The following topics describe how to extend the enterprise deployment domain with the Oracle SOA Suite software.

Variables Used When Extending the Domain with Oracle SOA Suite
: As you perform the tasks in this chapter, you will be referencing the directory variables listed in this section.

Synchronizing the System Clocks
: Before you extend the domain to include Oracle SOA Suite, verify that the system clocks on each host computer are synchronized. You can do this by running the `date` command as simultaneously as possible on the hosts in each cluster.

Installing the Software for an Enterprise Deployment
: The following sections describe how to install the software for an enterprise deployment.

Creating the Oracle SOA Suite Database Schemas
: Before you can configure an Oracle SOA Suite domain, you must install the required schemas in a certified database for use with this release of Oracle Fusion Middleware.

Extending the Enterprise Deployment Domain with Oracle SOA Suite
: This section provides instructions for extending the existing enterprise deployment domain with the Oracle SOA Suite software.

Configuring a Default Persistence Store for Transaction Recovery
: Each Managed Server uses a transaction log that stores information about committed transactions that are coordinated by the server and that may not have been completed. Oracle WebLogic Server uses this transaction log for recovery from system crashes or network failures. To leverage the migration capability of the Transaction Recovery Service for the Managed Servers within a cluster, store the transaction log in a location accessible to each Managed Server and its backup server.

Propagating the Extended Domain to the Domain Directories and Machines

Restarting and Validating Pre-existing Managed Servers

Modifying the Upload and Stage Directories to an Absolute Path
: After configuring the domain and unpacking it to the Managed Server domain directories on all the hosts, verify and update the `upload` and `stage` directories for the new Managed Servers.

## 15.1 Variables Used When Extending the Domain with Oracle SOA Suite

As you perform the tasks in this chapter, you will be referencing the directory variables listed in this section.

The values for several directory variables are defined in File System and Directory Variables Used in This Guide.

- ORACLE_HOME
- ASERVER_HOME
- MSERVER_HOME
- APPLICATION_HOME
- DEPLOY_PLAN_HOME
- OHS_DOMAIN_HOME
- JAVA_HOME
- ORACLE_RUNTIME

In addition, you'll be referencing the following virtual IP (VIP) address defined in Reserving the Required IP Addresses for an Enterprise Deployment:

- ADMINVHN

Actions in this chapter will be performed on the following host computers:

- WCPHOST1

- WCPHOST2
- WEBHOST1
- WEBHOST2
- WCCHOST1
- WCCHOST2

## 15.2 Synchronizing the System Clocks

Before you extend the domain to include Oracle SOA Suite, verify that the system clocks on each host computer are synchronized. You can do this by running the `date` command as simultaneously as possible on the hosts in each cluster.

Alternatively, there are third-party and open-source utilities you can use for this purpose.

## 15.3 Installing the Software for an Enterprise Deployment

The following sections describe how to install the software for an enterprise deployment.

Starting the Oracle SOA Suite Installer on WCPHOST1

Navigating the Installation Screens

Verifying the Installation

Installing Oracle SOA Suite on the Other Host Computers

### 15.3.1 Starting the Oracle SOA Suite Installer on WCPHOST1

To start the installation program:

1. Log in to WCPHOST1.
2. Go to the directory where you downloaded the installation program.
3. Launch the installation program by invoking the `java` executable from the JDK directory on your system, as shown in the example below.

   ```
   JAVA_HOME/bin/java -d64 -jar fmw_12.2.1.0.0_soa.jar
   ```

   Be sure to replace the JDK location in these examples with the actual JDK location on your system.

   For information about downloading the software and locating the actual installer file name for your product, see Identifying and Obtaining Software Downloads for an Enterprise Deployment.

When the installation program appears, you are ready to begin the installation.

### 15.3.2 Navigating the Installation Screens

The installation program displays a series of screens, in the order listed in the following table.

If you need additional help with any of the installation screens, click the screen name.

| Screen | Description |
|---|---|
| Welcome | This screen introduces you to the product installer. |
| Auto Updates | Use this screen to automatically search My Oracle Support for available patches or automatically search a local directory for patches that you've already downloaded for your organization. |
| Installation Location | Use this screen to specify the location of your Oracle home directory.<br>For more information about Oracle Fusion Middleware directory structure, see Selecting Directories for Installation and Configuration in *Planning an Installation of Oracle Fusion Middleware*. |
| Installation Type | Use this screen to select the type of installation and consequently, the products and feature sets you want to install.<br>• Select **SOA Suite** |
| Prerequisite Checks | This screen verifies that your system meets the minimum necessary requirements.<br>Roadmap for Verifying Your System Environment section in *Installing and Configuring the Oracle Fusion Middleware Infrastructure*. |
| Installation Summary | Use this screen to verify the installation options you selected.<br>Click **Install** to begin the installation. |
| Installation Progress | This screen allows you to see the progress of the installation.<br>Click **Next** when the progress bar reaches 100% complete. |
| Installation Complete | Review the information on this screen, then click **Finish** to dismiss the installer. |

## 15.3.3 Verifying the Installation

After you complete the installation, you can verify it by successfully completing the following tasks.

Reviewing the Installation Log Files

Checking the Directory Structure

Viewing the Contents of Your Oracle Home

### 15.3.3.1 Reviewing the Installation Log Files

Review the contents of the installation log files to make sure that no problems were encountered. For a description of the log files and where to find them, see "Understanding Installation Log Files" in *Installing Software with the Oracle Universal Installer*.

### 15.3.3.2 Checking the Directory Structure

The contents of your installation vary based on the options you selected during the installation.

The addition of Oracle SOA Suite adds the following directory and sub-directories:

```
/u01/oracle/products/fmw/soa

aiafp
bam
bin
bpm
common
integration
jlib
plugins
readme.txt
reports
soa
```

For more information about the directory structure you should see after installation, see "What are the Key Oracle Fusion Middleware Directories?" in *Understanding Oracle Fusion Middleware*.

#### 15.3.3.3 Viewing the Contents of Your Oracle Home

You can also view the contents of your Oracle home using the `viewInventory` script. For more information, see "Viewing the contents of an Oracle home" in *Installing Software with the Oracle Universal Installer*.

### 15.3.4 Installing Oracle SOA Suite on the Other Host Computers

If you have configured a separate shared storage volume or partition for the products mount point and *ORACLE_HOME* on WCCHOST2, then you must also perform the product installation on WCCHOST2.

For more information, see Shared Storage Recommendations When Installing and Configuring an Enterprise Deployment.

To install the software on the other host computers in the topology, log in to each host, and use the instructions in Starting the Infrastructure Installer on WCPHOST1 and Navigating the Infrastructure Installation Screens to create the Oracle home on the appropriate storage device.

---

**Note:**

In previous releases, the recommended enterprise topology included a colocated set of Oracle HTTP Server instances. In those releases, there was a requirement to install the Infrastructure on the Web Tier hosts (WEBHOST1 and WEBHOST2). However, for this release, the enterprise deployment topology assumes the Web servers are installed and configured in standalone mode, so they are not considered part of the application tier domain. For more information, see Configuring the Web Tier for an Enterprise Deployment

---

## 15.4 Creating the Oracle SOA Suite Database Schemas

Before you can configure an Oracle SOA Suite domain, you must install the required schemas in a certified database for use with this release of Oracle Fusion Middleware.

Starting the Repository Creation Utility (RCU)

Navigating the RCU Screens to Create the Schemas

Configuring SOA Schemas for Transactional Recovery

### 15.4.1 Starting the Repository Creation Utility (RCU)

To start the Repository Creation Utility (RCU):

1. Navigate to the *ORACLE_HOME*/oracle_common/bin directory on your system.
2. Make sure the *JAVA_HOME* environment variable is set to the location of a certified JDK on your system. The location should be up to but not including the bin directory. For example, if your JDK is located in /u01/oracle/products/jdk:

   On UNIX operating systems:

   ```
   export JAVA_HOME=/u01/oracle/products/jdk
   ```

3. Start RCU:

   On UNIX operating systems:

   ```
   ./rcu
   ```

### 15.4.2 Navigating the RCU Screens to Create the Schemas

Schema creation involves the following tasks:

- Task 1, "Introducing RCU"
- Task 2, "Selecting a Method of Schema Creation"
- Task 3, "Providing Database Connection Details"
- Task 4, "Specifying a Custom Prefix and Selecting Schemas"
- Task 5, "Specifying Schema Passwords"
- Task 6, "Specifying Custom Variables"
- Task 7, "Verifying the Tablespaces for the Required Schemas"
- Task 8, "Completing Schema Creation"
- Task 9, "Verifying the Schema Creation"

**Task 1 Introducing RCU**
Click **Next**.

**Task 2 Selecting a Method of Schema Creation**
If you have the necessary permission and privileges to perform DBA activities on your database, select **System Load and Product Load**. This procedure assumes that you have the necessary privileges.

If you do not have the necessary permission or privileges to perform DBA activities in the database, you must select **Prepare Scripts for System Load** on this screen. This option will generate a SQL script, which can be provided to your database administrator to create the required schema. See "Understanding System Load and Product Load" in *Creating Schemas with the Repository Creation Utility*.

**Task 3 Providing Database Connection Details**
Provide the database connection details for RCU to connect to your database.

In the **Host Name** field, enter the SCAN address of the Oracle RAC Database.

Enter the **DBMS/Service** details.

Enter the **Schema Owner** and **Schema Password** details.

Click **Next** to proceed, then click **OK** on the dialog window confirming that connection to the database was successful.

**Task 4 Specifying a Custom Prefix and Selecting Schemas**
Choose **Select existing prefix**, and then select the prefix you used when you created the initial domain.

From the list of schemas, select the **SOA Suite** schema. This will automatically select **SOA Infrastructure**. In addition, the following dependent schemas have already been installed with the Infrastructure and are grayed out:

- **Metadata Services**
- **Audit Services**
- **Audit Services Append**
- **Audit Services Viewer**
- **Oracle Platform Security Services**
- **User Messaging Service**

The custom prefix is used to logically group these schemas together for use in this domain only; you must create a unique set of schemas for each domain as schema sharing across domains is not supported.

> **Tip:**
> For more information about custom prefixes, see "Understanding Custom Prefixes" in *Creating Schemas with the Repository Creation Utility*.
>
> For more information about how to organize your schemas in a multi-domain environment, see "Planning Your Schema Creation" in *Creating Schemas with the Repository Creation Utility*.

Click **Next** to proceed, then click **OK** on the dialog window confirming that prerequisite checking for schema creation was successful.

**Task 5 Specifying Schema Passwords**
Specify how you want to set the schema passwords on your database, then specify and confirm your passwords.

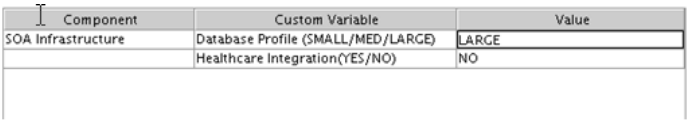
> **Tip:**
> You must make a note of the passwords you set on this screen; you will need them later on during the domain creation process.

**Task 6 Specifying Custom Variables**
Specify the custom variables for the SOA Infrastructure schema.

For the enterprise deployment topology, enter LARGE for the **Database Profile** custom variable.

If you are planning on using Oracle Healthcare, then enter YES for the **Healthcare Integration** variable.

For more information, see "About the Custom Variables Required for the SOA Suite Schemas" in *Installing and Configuring Oracle SOA Suite and Business Process Management*.



| Component | Custom Variable | Value |
|---|---|---|
| SOA Infrastructure | Database Profile (SMALL/MED/LARGE) | LARGE |
| | Healthcare Integration(YES/NO) | NO |

**Task 7 Verifying the Tablespaces for the Required Schemas**

On the Map Tablespaces screen, review the information, and then click **Next** to accept the default values.

Click **OK** in the confirmation dialog box.

**Task 8 Completing Schema Creation**

Navigate through the remainder of the RCU screens to complete schema creation. When you reach the Completion Summary screen, click **Close** to dismiss RCU.

**Task 9 Verifying the Schema Creation**

To verify that the schemas were created successfully, and to verify the database connection details, use SQL*Plus or another utility to connect to the database, using the SOAINFRA schema name and the password you provided.

For example:

```
./sqlplus

SQL*Plus: Release 11.2.0.4.0 Production on Fri Nov 1 08:44:18 2013

Copyright (c) 1982, 2013, Oracle.  All rights reserved.

Enter user-name: FMW1221_SOAINFRA
Enter password: soainfra_password

Connected to:
Oracle Database 11g Enterprise Edition Release 11.2.0.4.0 - 64bit Production
With the Partitioning, OLAP, Data Mining and Real Application Testing options

SQL>
```

## 15.4.3 Configuring SOA Schemas for Transactional Recovery

After you have installed the Oracle SOA Suite schemas successfully, use the procedure in this section to configure the schemas for transactional recovery.

This procedure sets the appropriate database privileges so that the Oracle WebLogic Server transaction manager can query the schemas for transaction state information and issue the appropriate commands, such as commit and rollback, during recovery of in-flight transactions after a WebLogic Server is unexpectedly unavailable.

These privileges should be granted to the owner of the SOAINFRA schema, which you defined when you created the schemas with the Repository Creation Utility.

To configure the SOA schemas for transactional recovery privileges:

1. Log on to SQL*Plus as a user with sysdba privileges. For example:

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

2. Enter the following commands:

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

Grant succeeded.

SQL> Grant force any transaction to soa_schema_prefix_soainfra;

Grant succeeded.

SQL>
```

## 15.5 Extending the Enterprise Deployment Domain with Oracle SOA Suite

This section provides instructions for extending the existing enterprise deployment domain with the Oracle SOA Suite software.

Extending the domain involves the following tasks.

Starting the Configuration Wizard

Navigating the Configuration Wizard Screens to Extend the Domain with Oracle SOA Suite

### 15.5.1 Starting the Configuration Wizard

To start the Configuration Wizard:

1. Shut down the domain completely before extending the domain. From the WebLogic Server Console, stop all managed servers and verify, and then stop the Administration Server.

2. Navigate to the following directory and start the WebLogic Server Configuration Wizard.

```
cd ORACLE_HOME/oracle_common/common/bin
./config.sh
```

### 15.5.2 Navigating the Configuration Wizard Screens to Extend the Domain with Oracle SOA Suite

Follow the instructions in this section to create and configure the domain for the topology.

---

**Note:**

You can use the same procedure described in this section to extend an existing domain. If your needs do not match the instructions given in the procedure, be sure to make your selections accordingly, or refer to the supporting documentation for additional details.

---

Domain creation and configuration includes the following tasks.

- Task 1, "Selecting the Domain Type and Domain Home Location"
- Task 2, "Selecting the Configuration Template"
- Task 3, "Specifying the Database Configuration Type"
- Task 4, "Specifying JDBC Component Schema Information"
- Task 5, "Providing the GridLink Oracle RAC Database Connection Details"
- Task 6, "Testing the JDBC Connections"
- Task 8, "Selecting Advanced Configuration"
- Task 9, "Configuring Managed Servers"
- Task 10, "Configuring a Cluster"
- Task 11, "Assigning Managed Servers to the Cluster"
- Task 12, "Configuring Coherence Clusters"
- Task 13, "Verifying the Existing Machines"
- Task 14, "Assigning Servers to Machines"
- Task 17, "Configuring the JMS File Store"
- Task 18, "Reviewing Your Configuration Specifications and Configuring the Domain"
- Task 19, "Writing Down Your Domain Home and Administration Server URL"
- Task 20, "Start the Administration Server"

**Task 1 Selecting the Domain Type and Domain Home Location**

On the Configuration Type screen, select **Update an existing domain**.

In the **Domain Location** field, select the value of the *ASERVER_HOME* variable, which represents the complete path to the Administration Server domain home you created when you created the initial domain.

Do not enter the value of the *MSERVER_HOME* variable, which represents the location of the Managed Servers domain directory.

For more information about the directory location variables, see File System and Directory Variables Used in This Guide

> **Tip:**
> More information about the other options on this screen can be found in Configuration Type in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 2 Selecting the Configuration Template**

On the Templates screen, make sure **Update Domain Using Product Templates** is selected, then select the following templates:

- **Oracle SOA Suite - 12.2.1.1.0 [soa]**

**Tip:**
More information about the options on this screen can be found in Templates in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 3 Specifying the Database Configuration Type

On the Database Configuration Type screen, select **RCU Data**.

All fields are pre-populated, because you already configured the domain to reference the Fusion Middleware schemas that are required for the Infrastructure domain.

Verify and ensure that credentials in all the fields are the same that you have provided while configuring Oracle Fusion Middleware Infrastructure.

Click **Get RCU Configuration** after you finish verifying the database connection information. The following output in the Connection Result Log indicates that the operating succeeded:

```
Connecting to the database server...OK
Retrieving schema data from database server...OK
Binding local schema components with retrieved data...OK

Successfully Done.
```

**Tip:**
For more information about the **RCU Data** option, see "Understanding the Service Table Schema" in *Creating Schemas with the Repository Creation Utility*.

For more information about the other options on this screen, see "Datasource Defaults" in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 4 Specifying JDBC Component Schema Information

On the JDBC Component Schema screen, select all the SOA schemas in the table.

When you select the schemas, the fields on the page are activated and the database connection fields are populated automatically.

Click **Convert to GridLink** and click **Next**.

### Task 5 Providing the GridLink Oracle RAC Database Connection Details

On the GridLink Oracle RAC Component Schema screen, provide the information required to connect to the RAC database and component schemas, as shown in the following table.

| Element | Description and Recommended Value |
|---|---|
| SCAN, Host Name, and Port | Select the **SCAN** check box.<br>In the **Host Name** field, enter the Single Client Access Name (SCAN) Address for the Oracle RAC database.<br>In the **Port** field, enter the SCAN listening port for the database (for example, `1521`) |
| ONS Host and Port | In the **ONS Host** field, enter the SCAN address for the Oracle RAC database.<br>In the **Port** field, enter the ONS Remote port (typically, `6200`). |

| Element | Description and Recommended Value |
|---|---|
| Enable Fan | Verify that the **Enable Fan** check box is selected, so the database can receive and process FAN events. |

### Task 6 Testing the JDBC Connections

Use the JDBC Component Schema Test screen to test the data source connections you have just configured.

A green check mark in the **Status** column indicates a successful test. If you encounter any issues, see the error message in the Connection Result Log section of the screen, fix the problem, then try to test the connection again.

> **Tip:**
> For more information about the other options on this screen, see "Test Component Schema" in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 7 Keystore

Use this screen to specify details about the keystore to be used in the domain.

For a typical enterprise deployment, you can leave the default values.

For more information, see Keystore in *Creating WebLogic Domains Using the Configuration Wizard*.

### Task 8 Selecting Advanced Configuration

To complete domain configuration for the topology, select the following options on the Advanced Configuration screen:

- **Topology**
- **File Store**

### Task 9 Configuring Managed Servers

On the Managed Servers screen, a new Managed Server for Oracle SOA Suite appears in the list of servers. This server was created automatically by the Oracle SOA Suite configuration template you selected in Task 2, "Selecting the Configuration Template".

Perform the following tasks to modify the default Oracle SOA Suite Managed Server and create a second Oracle SOA Suite Managed Server:

1. Rename the default Oracle SOA Suite Managed Server to `WLS_SOA1`.
2. Click **Add** to create a new Oracle SOA Suite Managed Server, and name it `WLS_SOA2`.

   > **Tip:**
   > The server names recommended here will be used throughout this document; if you choose different names, be sure to replace them as needed.

3. Use the information in the following table to fill in the rest of the columns for each Oracle SOA Suite Managed Server.

**Tip:**
More information about the options on the Managed Server screen can be found in Managed Servers in *Creating WebLogic Domains Using the Configuration Wizard*.

| Server Name | Listen Address | Listen Port | Enable SSL | SSL Listen Port | Server Groups |
|---|---|---|---|---|---|
| WLS_SOA1 | WCCHOST1 | 8001 | No | Disabled | SOA-MGD-SVRS-ONLY |
| WLS_SOA2 | WCCHOST2 | 8001 | No | Disabled | SOA-MGD-SVRS-ONLY |

**Task 10 Configuring a Cluster**
In this task, you create a cluster of Managed Servers to which you can target the Oracle SOA Suite software.

Use the Clusters screen to create a new cluster:

1. Click the **Add** button.
2. Specify `SOA_Cluster` in the **Cluster Name** field.

**Note:**
By default, server instances in a cluster communicate with one another using unicast. If you want to change your cluster communications to use multicast, refer to "Considerations for Choosing Unicast or Multicast" in *Administering Clusters for Oracle WebLogic Server*.

**Tip:**
More information about the options on this screen can be found in Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 11 Assigning Managed Servers to the Cluster**
Use the Assign Servers to Clusters screen to assign `WLS_SOA1` and `WLS_SOA2` to the new cluster `SOA_Cluster`:

1. In the Clusters pane, select the cluster to which you want to assign the servers; in this case, `SOA_Cluster`.
2. In the Servers pane, assign `WLS_SOA1` to `SOA_Cluster` by doing one of the following:
   - Click `WLS_SOA1` Managed Server once to select it, and then click on the right arrow to move it beneath the selected cluster in the Clusters pane.
   - Double-click `WLS_SOA1` to move it beneath the selected cluster in the clusters pane.
3. Repeat to assign `WLS_SOA2` to `SOA_Cluster`.

**Tip:**
More information about the options on this screen can be found in Assign Servers to Clusters in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 12 Configuring Coherence Clusters**
Use the Coherence Clusters screen to configure the Coherence cluster that is automatically added to the domain. Leave the port number value at `9991`, as it was defined during the initial Infrastructure domain creation.

**Note:**
For Coherence licensing information, refer to "Oracle Coherence" in *Oracle Fusion Middleware Licensing Information*.

**Task 13 Verifying the Existing Machines**
Click **Next** to proceed.

**Task 14 Assigning Servers to Machines**
Use the Assign Servers to Machines screen to assign the Oracle SOA Suite Managed Servers you just created to the corresponding machines in the domain.

Assign `WLS_SOA1` to `WCCHOST1`, and assign `WLS_SOA2` to WCCHOST2.

**Tip:**
More information about the options on this screen can be found in Assign Servers to Machines in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 15 Configuring Virtual Targets**
Click **Next** to proceed to the next screen.

**Task 16 Configuring Partitions**
Click **Next** to proceed to the next screen.

**Task 17 Configuring the JMS File Store**
In the JMS File Stores screen, assign the following directory for each of the SOA Persistence stores, including UMS and BPM file stores:

```
ORACLE_RUNTIME/domain_name/SOA_cluster/jms
```

In this example, replace *ORACLE_RUNTIME* with the value of the variable for your environment. Replace *domain_name* with the name you assigned to the domain.

Replace `SOA_cluster` with the name you assigned to the cluster.

**Task 18 Reviewing Your Configuration Specifications and Configuring the Domain**

The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any previous screen if you need to make any changes, either by using the **Back** button or by selecting the screen in the navigation pane.

Domain creation will not begin until you click **Update**.

> **Tip:**
> More information about the options on this screen can be found in Configuration Summary in *Creating WebLogic Domains Using the Configuration Wizard*.

**Task 19 Writing Down Your Domain Home and Administration Server URL**

The Configuration Success screen will show the following items about the domain you just configured, including:

- Domain Location
- Administration Server URL

Make a note of both these items, because you will need them later; you will need the domain location to access the scripts used to start the Administration Server, and you will need the Administration Server URL to access the WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control.

Click **Finish** to dismiss the configuration wizard.

**Task 20 Start the Administration Server**

Start the Administration Server to ensure the changes you have made to the domain have been applied.

## 15.6 Configuring a Default Persistence Store for Transaction Recovery

Each Managed Server uses a transaction log that stores information about committed transactions that are coordinated by the server and that may not have been completed. Oracle WebLogic Server uses this transaction log for recovery from system crashes or network failures. To leverage the migration capability of the Transaction Recovery Service for the Managed Servers within a cluster, store the transaction log in a location accessible to each Managed Server and its backup server.

**Note:**

To enable migration of the Transaction Recovery Service, specify a location on a persistent storage solution that is available to other servers in the cluster. All Managed Servers in the cluster must be able to access this directory. This directory must also exist before you restart the server.

The recommended location is a dual-ported SCSI disk or on a Storage Area Network (SAN). Note that it is important to set the appropriate replication and backup mechanisms at the storage level to guarantee protection in cases of a storage failure.

This information applies for file-based transaction logs. You can also configure a database-based persistent store for translation logs. For more information, see Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment.

To set the location for the default persistence stores:

1. Log into the Oracle WebLogic Server Administration Console:

   `ADMINVHN:7001/console`

2. In the Change Center section, click **Lock & Edit**.

3. For each of the Managed Servers in the cluster:

   a. In the Domain Structure window, expand the **Environment** node, and then click the **Servers** node.

      The Summary of Servers page appears.

   b. Click the name of the server (represented as a hyperlink) in **Name** column of the table.

      The settings page for the selected server appears and defaults to the Configuration tab.

   c. On the Configuration tab, click the **Services** tab.

   d. In the Default Store section of the page, enter the path to the folder where the default persistent stores will store its data files.

      For the enterprise deployment, use the *ORACLE_RUNTIME* directory location. This subdirectory serves as the central, shared location for transaction logs for the cluster. For more information, see File System and Directory Variables Used in This Guide.

      For example:

      `ORACLE_RUNTIME/domain_name/cluster_name/tlogs`

      In this example, replace *ORACLE_RUNTIME* with the value of the variable for your environment. Replace *domain_name* with the name you assigned to the domain. Replace *cluster_name* with the name of the cluster you just created.

   e. Click **Save**.

4. Complete step 3 for all servers in the SOA_Cluster.

5. Click **Activate Changes**.
6. Complete steps 1 through 5 for the other servers in the cluster.

**Note:**

You will validate the location and the creation of the transaction logs later in the configuration procedure.

## 15.7 Propagating the Extended Domain to the Domain Directories and Machines

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 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 WCPHOST1 to create a template pack:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true
          -domain=ASERVER_HOME
          -template=/full_path/wcpdomaintemplateExtSOA.jar
          -template_name=wcp_domain_template_extension_soa
```

In this example:

- Replace *ASERVER_HOME* with the actual path to the domain directory you created on the shared storage device.
- Replace *full_path* with the complete path to the directory where you want the template jar file saved.
- `wcpdomaintemplateExtSOA.jar` is a sample name for the JAR file you are creating, which will contain the domain configuration files, including the configuration files for the Oracle HTTP Server instances.
- `wcp_domain_template_extension_soa` is the name assigned to the domain template file.

3. Run the following `unpack` command on WCPHOST1 to propagate the template created in the preceding step to the *MSERVER_HOME* directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME
            -template=/full_path/wcpdomaintemplateExtSOA.jar
            -app_dir=APPLICATION_HOME
            -overwrite_domain=true
```

In this example:

- Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
- `wcpdomaintemplateExtSOA.jar` is the directory path and name of the template you created when you ran the pack command to pack up the domain on the shared storage device.
- The `-overwrite_domain=true` argument is necessary when you are 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.
- Replace *`APPLICATION_HOME`* with the complete path to the Application directory for the domain on local storage.

  **Tip:**

  For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

4. Run the following command on WCPHOST1 to copy the template pack created in step 1 to WCPHOST2, WCCHOST1, and WCCHOST2:

```
scp /full_path/wcpdomaintemplateExtSOA.jar oracle@WCPHOST2:/full_path/
scp /full_path/wcpdomaintemplateExtSOA.jar oracle@WCCHOST1:/full_path/
scp /full_path/wcpdomaintemplateExtSOA.jar oracle@WCCHOST2:/full_path/
```

5. Run the following `unpack` command on each of the remote hosts to deploy the domain template copied in the preceding step to the *MSERVER_HOME* directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME
            -template=/full_path/wcpdomaintemplateExtSOA.jar
            -app_dir=APPLICATION_HOME
            -overwrite_domain=true
```

   In this example:

   - Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
   - `wcpdomaintemplateExtSOA.jar`is the directory path and name of the template you created when you ran the pack command to pack up the domain on the shared storage device.
   - The `-overwrite_domain=true` argument is necessary when you are 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.

- Replace *APPLICATION_HOME* with the complete path to the Application directory for the domain on local storage.

  **Tip:**

  For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

## 15.8 Restarting and Validating Pre-existing Managed Servers

Restart the managed servers for the pre-existing components now that the domain has been extended and unpacked to the *MSERVER_HOME* directories on all of the servers.

1. From the WebLogic Server Console, restart the WLS_WSM*n* Managed Servers for the WebServices Manager Policy Manager.
2. From another browser window, verify the WSM-PM application is responding by successfully loading the URL:

   ```
   http://wcpinternal.example.com/wsm-pm/validator
   ```

3. Start other pre-existing managed servers as necessary. Other product functionality will not be needed at this stage.

## 15.9 Modifying the Upload and Stage Directories to an Absolute Path

After configuring the domain and unpacking it to the Managed Server domain directories on all the hosts, verify and update the `upload` and `stage` directories for the new Managed Servers.

This step is necessary to avoid potential issues when performing remote deployments and for deployments that require the stage mode.

To update these directory paths for all the Managed Servers in the Managed Server domain home directory:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the left navigation tree, expand **Domain**, and then **Environment**.
3. Click **Lock & Edit**.
4. Click **Servers**.
5. For each new Managed Server in the Managed Server domain home directory:
   a. Click the name of the Managed Server.
   b. Click the **Configuration** tab, and then click the **Deployment** tab.
   c. Verify that the **Staging Directory Name** is set to the following:

      ```
      MSERVER_HOME/servers/server_name/stage
      ```

      Replace *MSERVER_HOME* with the directory path for the MSERVER_HOME directory; replace *server_name* with the name of the Server you are editing.

   d. Update the **Upload Directory Name** to the following value:

`ASERVER_HOME`/servers/AdminServer/upload

Replace *ASERVER_HOME* with the directory path for the ASERVER_HOME directory.

e. Click **Save**.

f. Return to the Summary of Servers screen.

6. When you have modified these values for each Managed Server, click **Activate Changes**.

## 15.10 Starting and Validating the WLS_SOA1 Managed Server

Now that you have extended the domain, started the Administration Server, and propagated the domain to the other hosts, you can start the newly configured Oracle SOA Suite Managed Servers.

This process involves three tasks as described in the following sections.

Starting the WLS_SOA1 Managed Server

Adding the SOAAdmin Role to the Administrators Group

Validating the Managed Server by Logging in to the SOA Infrastructure

### 15.10.1 Starting the WLS_SOA1 Managed Server

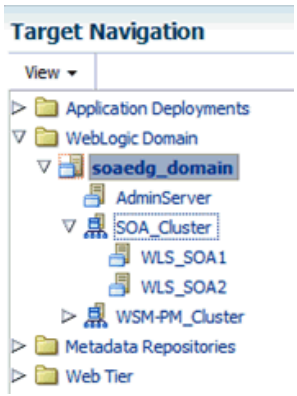
To start the WLS_SOA1 Managed Server:

1. Enter the following URL into a browser to display the Fusion Middleware Control login screen:

   `http://ADMINVHN:7001/em`

2. Log in to Fusion Middleware Control using the Administration Server credentials.

3. In the **Target Navigation** pane, expand the domain to view the Managed Servers in the domain.




4. Select only the **WLS_SOA1** Managed Server and click **Start Up** on the Oracle WebLogic Server toolbar.

**Note:**

SOA Servers depend on the policy access service to be functional. This implies that the WSM-PM Managed Servers in the domain need to be up and running and reachable before the SOA servers are started.

5. When the startup operation is complete, navigate to the Domain home page and verify that the WLS_SOA1 Managed Server is up and running.

### 15.10.2 Adding the SOAAdmin Role to the Administrators Group

Before you validate the Oracle SOA Suite configuration on the WLS_SOA1 Managed Server, add the `SOAAdmin` administration role to the enterprise deployment administration group (`WCPAdministrators`).

To perform this task, refer to Configuring Roles for Administration of an Enterprise Deployment.

### 15.10.3 Validating the Managed Server by Logging in to the SOA Infrastructure

After you add the `SOAAdmin` role to the SOA Administrators group, you can then validate the configuration of the Oracle SOA Suite software on the WLS_SOA1 Managed Server as follows:

1. Use your Web browser to navigate to the following URL:

   `http://WCCHOST1:8001/soa-infra/`

2. Log in using the enterprise deployment administrator user credentials (`weblogic_wcp`).

   You should see a web page with the following title:

   `"Welcome to the Oracle SOA Platform on WebLogic"`

## 15.11 Starting and Validating the WLS_SOA2 Managed Server

After you have validated the successful configuration and startup of the WLS_SOA1 Managed Server, you can then start and validate the WLS_SOA2 Managed Server.

To start and validate the WLS_SOA2 Managed Server, use the procedure in Starting and Validating the WLS_SOA1 Managed Serverfor WLS_SOA2 Managed Server.

For the validation URL, enter the following URL in your web browser and log in using the enterprise deployment administrator user (`weblogic_soa`):

`http://WCCHOST2:8001/soa-infra/`

## 15.12 Validating the Location and Creation of the Transaction Logs

After WLS_SOA1 and WLS_SOA2 are up and running, verify that the transaction log directory and transaction logs were created as expected.

Run the following command to verify, based on the steps you performed in Configuring a Default Persistence Store for Transaction Recovery:

`ORACLE_RUNTIME/domain_name/cluster_name/tlogs`

- `_WLS_WLS_SOA1000000.DAT`

- `_WLS_WLS_SOA2000000.DAT`

## 15.13 Configuring Oracle HTTP Server for the Extended Domain

The following sections describe how to configure the Oracle HTTP Server instances so they route requests for both public and internal URLs to the proper clusters in the enterprise topology.

Configuring Oracle HTTP Server for SOA in an Oracle WebCenter Portal Enterprise Deployment

Configuring the WebLogic Proxy Plug-In

Validating the Oracle SOA Suite URLs Through the Load Balancer

### 15.13.1 Configuring Oracle HTTP Server for SOA in an Oracle WebCenter Portal Enterprise Deployment

When integrating SOA with WebCenter Portal for workflow functionality both internal and end-user access to the SOA Suite resources should be configured.

Use the following procedure to configure the Oracle HTTP Server instances in the web tier, so they route requests correctly to the Oracle SOA Suite cluster. This procedure assumes that you have performed the Oracle HTTP Server configuration tasks described in Configuring Oracle HTTP Server to Route Requests to the Application Tier.

Configure the virtual host configuration files so that requests are routed properly to the Oracle SOA Suite clusters:

1. Log in to WEBHOST1 and change directory to the configuration directory for the first Oracle HTTP Server instance (`ohs1`):

   ```
   cd OHS_DOMAIN_HOME/config/fmwconfig/components/OHS/ohs1/moduleconf/
   ```

2. Edit the `wcpinternal_vh.conf` file and add the following directives inside the `<VirtualHost>` tags:

   **Note:**

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

```
# soa-infra
<Location /soa-infra>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# SOA inspection.wsil
<Location /inspection.wsil>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
```

```
    WLProxySSLPassThrough OFF
</Location>

# Worklist
<Location /integration>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# UMS prefs
<Location /sdpmessaging/userprefs-ui>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# Default to-do taskflow
<Location /DefaultToDoTaskFlow>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# Workflow
<Location /workflow>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

#Required if attachments are added for workflow tasks
 <Location /ADFAttachmentHelper>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# SOA composer application
 <Location /soa/composer>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

 <Location /frevvo>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>
</VirtualHost>
```

3. Edit the `wcp_vh.conf` file and add the following directives inside the `<VirtualHost>` tags:

**Note:**

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

```
# soa-infra
<Location /soa-infra>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# SOA inspection.wsil
<Location /inspection.wsil>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# Worklist
<Location /integration>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# UMS prefs
<Location /sdpmessaging/userprefs-ui>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# Default to-do taskflow
<Location /DefaultToDoTaskFlow>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# Workflow
<Location /workflow>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

#Required if attachments are added for workflow tasks
 <Location /ADFAttachmentHelper>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
```

```
      WLProxySSL ON
      WLProxySSLPassThrough ON
   </Location>

   # SOA composer application
    <Location /soa/composer>
      WLSRequest ON
      WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
      WLProxySSL ON
      WLProxySSLPassThrough ON
   </Location>

    <Location /frevvo>
      WLSRequest ON
      WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
      WLProxySSL ON
      WLProxySSLPassThrough ON
   </Location>
   </VirtualHost>
```

4. Copy the `wcpinternal_vh.conf`and `wcp_vh.conf` files to the configuration directory for the second Oracle HTTP Server instance (`ohs2`):

   *OHS_DOMAIN_HOME*`/config/fmwconfig/components/`**`ohs2`**`/moduleconf/`

5. Edit the `wcpinternal_vh.conf` and `wcp_vh.conf` to change any references to WEBHOST1 to WEBHOST2 in the `<VirtualHost>` directives.

6. Restart both Oracle HTTP servers.

***Example 15-1 Sample Content for the `wcpinternal_vh.conf` File***

> **Note:** The following sample configuration files content only includes SOA Suite and Oracle WebServices Manager resources. Resources for other products that may have been configured in prior chapters are not represented here.

```
<VirtualHost WEBHOST1:7777>
    ServerName http://wcpinternal.example.com:80
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit

# WSM-PM
<Location /wsm-pm>
     WebLogicCluster WCPHOST1:7010,WCPHOST2:7010
     WLSRequest ON
     WLProxySSL OFF
     WLProxySSLPassThrough OFF
</Location>

#soa-infra
<Location /soa-infra>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>
```

```
# SOA inspection.wsil
<Location /inspection.wsil>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# Worklist
<Location /integration>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# UMS prefs
<Location /sdpmessaging/userprefs-ui>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# Default to-do taskflow
<Location /DefaultToDoTaskFlow>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# Workflow
<Location /workflow>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

#Required if attachments are added for workflow tasks
 <Location /ADFAttachmentHelper>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

# SOA composer application
 <Location /soa/composer>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
</Location>

 <Location /frevvo>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL OFF
    WLProxySSLPassThrough OFF
```

```
</Location>
</VirtualHost>
```

***Example 15-2 Sample Content for the wcp_vh.conf File***

```
<VirtualHost WEBHOST1:7777>
    ServerName http://wcp.example.com:443
    ServerAdmin you@your.address
    RewriteEngine On
    RewriteOptions inherit

# WSM-PM
<Location /wsm-pm>
     WebLogicCluster WCPHOST1:7010,WCPHOST2:7010
     WLSRequest ON
     WLProxySSL ON
     WLProxySSLPassThrough ON
</Location>

#soa-infra
<Location /soa-infra>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# SOA inspection.wsil
<Location /inspection.wsil>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# Worklist
<Location /integration>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# UMS prefs
<Location /sdpmessaging/userprefs-ui>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# Default to-do taskflow
<Location /DefaultToDoTaskFlow>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# Workflow
<Location /workflow>
```

```
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

#Required if attachments are added for workflow tasks
 <Location /ADFAttachmentHelper>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

# SOA composer application
 <Location /soa/composer>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>

 <Location /frevvo>
    WLSRequest ON
    WebLogicCluster WCCHOST1:8001,WCCHOST2:8001
    WLProxySSL ON
    WLProxySSLPassThrough ON
</Location>
</VirtualHost>
```

## 15.13.2 Configuring the WebLogic Proxy Plug-In

Before you can validate that requests are routed correctly through the Oracle HTTP Server instances, you must set the `WebLogic Plug-In Enabled` parameter for the clusters you just configured.

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the **Domain Structure** pane, expand the **Environment** node.
3. Click **Clusters**.
4. Select the cluster to which you want to proxy requests from Oracle HTTP Server.

   The **Configuration: General** tab is displayed.
5. Scroll down to the **Advanced** section and expand it.
6. Click **Lock & Edit** in the Change Center.
7. Set **WebLogic Plug-In Enabled** to **yes**.
8. Click **Save** and click **Activate Changes**.
9. Click **Activate Changes** in the Change Center.
10. Restart all Managed Servers in all of the clusters that you modified in this chapter.

### 15.13.3 Validating the Oracle SOA Suite URLs Through the Load Balancer

To validate the configuration of the Oracle HTTP Server virtual hosts and to verify that the hardware load balancer can route requests through the Oracle HTTP Server instances to the application tier:

1. 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.

2. Verify that you can access these URLs:

   - `https://wcp.example.com:443/soa-infra`
   - `https://wcp.example.com:443/integration/worklistapp`
   - `https://wcp.example.com:443/sdpmessaging/userprefs-ui`
   - `https://wcp.example.com:443/soa/composer`

## 15.14 Post-Configuration Steps for Oracle SOA Suite

After you install and configure Oracle SOA Suite, consider the following post-configuration tasks.

Enabling SSL Communication Between the SOA Servers and the Hardware Load Balancer

Considerations for sync-async interactions in a SOA cluster

Setting the Front End Host and Port for the SOA Cluster
: You must set the front-end HTTP host and port for the Oracle WebLogic Server cluster hosting the Oracle SOA Suite servers. This can be done in the Configuration Wizard, while you are specifying the properties of the domain, but when you are adding a SOA Cluster as part of an Oracle WebCenter Portal enterprise deployment, it is recommended that you perform this task after you verify the SOA Managed Servers.

Updating the Workflow Front End Address for Appropriate Task Display
: You must configure Oracle Workflow with the appropriate URL so that the details of the Default-to-do tasks and custom tasks use the front-end load balancer to create the task-display URLs.

### 15.14.1 Enabling SSL Communication Between the SOA Servers and the Hardware Load Balancer

After you extend the domain with Oracle SOA Suite, you should also ensure that the Administration Server and Managed Servers can access the front-end, SSL URL of the hardware load balancer.

This will allow SOA Composite applications and web services to invoke callbacks and other communications with the front-end, secure URL.

For more information, see Enabling SSL Communication Between the Middle Tier and the Hardware Load Balancer.

### 15.14.2 Considerations for sync-async interactions in a SOA cluster

In a SOA cluster, the following scenarios are not supported:

- Synchronous BPEL process with mid-process receive.
- Synchronous BPEL process calling asynchronous services.
- Callback from synchronous processes.

### 15.14.3 Setting the Front End Host and Port for the SOA Cluster

You must set the front-end HTTP host and port for the Oracle WebLogic Server cluster hosting the Oracle SOA Suite servers. This can be done in the Configuration Wizard, while you are specifying the properties of the domain, but when you are adding a SOA Cluster as part of an Oracle WebCenter Portal enterprise deployment, it is recommended that you perform this task after you verify the SOA Managed Servers.

To set the front end host and port from the Weblogic Server Administration Console:

1. Log in to the WebLogic Server Administration Console.
2. In the Change Center, click **Lock & Edit**.
3. In the Domain Structure panel, expand **Environment**, and click **Clusters**.
4. On the Clusters page, click **SOA_Cluster** and then select the **HTTP** tab.
5. Set the following values:
   - **Frontend Host**: `wcp.example.com`
   - **Frontend HTTP Port**: `80`
   - **Frontend HTTPS Port**: `443`
6. Click **Save**.
7. Click **Activate Changes**.
8. Restart the WLS_SOA1 Managed Server.

### 15.14.4 Updating the Workflow Front End Address for Appropriate Task Display

You must configure Oracle Workflow with the appropriate URL so that the details of the Default-to-do tasks and custom tasks use the front-end load balancer to create the task-display URLs.

This process can be completed once and will take effect for all SOA servers.

To configure the appropriate URLs:

1. Log in to Oracle Enterprise Manager Fusion Middleware Control with the username and password you specified in the Updating the boot.properties File and Restarting the System section.
2. From the WebLogic Domain drop-down menu, select **System MBean Browser**.

3. In the Mbean navigation, expand **Application Defined MBeans** > **oracle.as.soainfra.config** > **Server: WLS_SOA1** > **WorkflowConfig**, and then click **human-workflow**.
4. In the **FusionAppsFrontendHostUrl** field, enter the following:

   ```
   *=https://wcp.example.com:443
   ```

5. Click **Apply**.

## 15.15 Enabling Automatic Service Migration and JDBC Persistent Stores for Oracle SOA Suite

To ensure that Oracle SOA Suite is configured for high availability, configure the Oracle SOA Suite Managed Servers for automatic service migration.

For more information on enabling automatic service migration, see Configuring Automatic Service Migration in an Enterprise Deployment.

For additional high availability, you can also configure your transaction logs store and JMS store in a database. For more information, see Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment.

# 16

# Integrating WebCenter Portal Workflows with Oracle SOA Suite in the Same Domain

WebCenter Portal provides several prebuilt workflows that handle portal membership notifications, portal subscription requests, and so on. WebCenter Portal workflows rely on the Oracle BPM Worklist, which is installed as a component of Oracle SOA Suite.

WebCenter Portal Worklist integration requires that the BPEL Services provided by SOA Suite share the same WebTier, SSO, and Identity Store with the portal. For this Enterprise Deployment Guide, SOA Suite is installed and configured in the same WebLogic Server Domain and included in the WebTier, SSO, and directory configurations.

For more information on Oracle BPM Worklist features, see Using Oracle BPM Worklist in *Developing SOA Applications with Oracle SOA Suite*.

The tasks that must be performed to enable the WebCenter Portal workflow functionality in WebCenter Portal are as follows.

> **Note:** Integrating BPM functionality into portal pages using the BPM Process Portal Resource Catalog requires additional steps not covered in this guide. For more information see Integrating BPM Functionality into WebCenter Portal.

Backing Up the Installation
: Back up the environment before re-configuring to include the Portal Workflow Integration with SOA Suite.

Installing Oracle SOA Suite

Installing the Oracle WebCenter Portal SOA Composites
: To use workflows in WebCenter Portal, you must install WebCenter Portal SOA Composites by using the portal installer after SOA Suite is installed.

Extending the Domain to Deploy the WebCenter Portal Workflows
: WebCenter Portal workflows are deployed to Oracle SOA Server. To prepare the SOA cluster for workflows, you must extend the domain in which Oracle SOA is installed by using the template `oracle.wc_composite_template.jar`.

Propagating the Extended Domain to the Domain Directories and Machines
: Propagate the start scripts and classpath configuration from the Administration Server's domain directory to the Managed Server domain directory.

Restoring customizations to setDomainEnv.sh after Unpacking the Domain
: If any customizations have been made earlier to the `setDomainEnv.sh` files in *ASERVER_HOME* and *MSERVER_HOME*, then these customizations will need to be repeated after any domain extension.

Updating the NodeManager Configuration After Unpacking the Domain
: When extending a domain after setting up custom keystores, certificates, and custom identity aliases, the `nodemanager.properties` file in *MSERVER_HOME* may be overwritten with some values from the `nodemanager.properties` file for *ASERVER_HOME*. Specifically, the `ListenAddress` and/or `CustomIdentityAlias` values can be reset.

Starting the Domain and Validating the WebCenter Portal SOA Composite Domain Extension
: Start the entire domain and use Enterprise Manager to verify the deployment of the Portal SOA Composites and WebCenter Worklist Detail application.

Configuring WS-Security for Oracle SOA and WebCenter Portal
: WebCenter Portal Web services, deployed to Oracle WebCenter Portal, facilitate communication between WebCenter Portal and the SOA server. You must secure these Web service calls.

Verifying Application Roles
: Before you configure WebCenter Portal with SOA Suite, understand and verify the `SOAAdmin` and `BPMWorkflowAdmin` application roles.

Creating the Connection to the BPEL Server
: WebCenter Portal uses BPEL server to host internal workflows, such as worklists, membership notifications, subscription requests, and so on. BPEL Services are configured on the SOA Managed Servers. To enable workflow functionality for WebCenter Portal, a connection to the BPEL service is required.

Validating the Connection to the BPEL Server
: After you create the connection to the BPEL Server, validate the connection to be sure it is working properly.

Configuring WebCenter Portal Workflow Notifications to be Sent by Email
: WebCenter Portal can use human workflows (requiring human interaction), which are integrated with SOA workflows. The SOA server can configure email so that notifications are delivered to a user's inbox, where the user can accept or reject the notification.

Testing the Oracle BPM Worklist Application in WebCenter Portal
: Testing of the WebCenter Portal invitation and membership workflows and email notifications can be performed using end-user accounts and requires specific portal run-time configuration to set up the test case.

## 16.1 Backing Up the Installation

Back up the environment before re-configuring to include the Portal Workflow Integration with SOA Suite.

This is a quick backup for the express purpose of immediate restore in case of problems in the further steps. The backup destination is the local disk. You can discard this backup once the enterprise deployment setup is complete. At that point, the regular deployment-specific backup and recovery process can be initiated. The Oracle Fusion Middleware Administrator's Guide provides further details.

To back up the environment:

1. Shutdown the domain resources in order: Managed Servers, Admin Server, Node Managers.
2. Back up the database. Perform a full database backup (either hot or cold) using Oracle Recovery Manager (recommended).
3. Clear the WebLogic Server logs to aid in troubleshooting this chapter and reduce backup size (optional).

```
cd ASERVER_HOME
find ./servers/AdminServer/logs -type f ! -size 0c -print -exec rm -f {} \+
cd MSERVER_HOME
find ./servers/*/logs -type f ! -size 0c -print -exec rm -f {} \+
```

4. Backup up the Administration Server domain directory.

```
cd ASERVER_HOME
cd ..
tar -czf ./ASERVER_HOME-domain_name.chapter19.1.tgz ./domain_name
```

5. Back up the Applications Directory.

```
cd APPLICATION_HOME
cd ..
tar -czf ./APPLICATION_HOME-domain_name.chapter19.1.tgz ./domain_name
```

6. Restart the Node Managers for *ASERVER_HOME* and *MSERVER_HOME*.

```
cd ASERVER_HOME/bin
nohup ./startNodeManager.sh > ASERVER_HOME/nodemanager/nodemanager.out 2>&1 &
cd MSERVER_HOME/bin
nohup ./startNodeManager.sh > MSERVER_HOME/nodemanager/nodemanager.out 2>&1 &
```

## 16.2 Installing Oracle SOA Suite

To support workflows, WebCenter Portal relies on the BPEL server, which is included with Oracle SOA Suite. For information about installing Oracle SOA Suite as part of this domain, see Extending the Domain with Oracle SOA Suite .

## 16.3 Installing the Oracle WebCenter Portal SOA Composites

To use workflows in WebCenter Portal, you must install WebCenter Portal SOA Composites by using the portal installer after SOA Suite is installed.

During the initial installation, the Extending the Domain with Oracle WebCenter Portal section included an option to select the Portal SOA Composites. If the option was selected, then proceed to the Extending the Domain to Deploy the WebCenter Portal Workflows section.

To install WebCenter Portal SOA Composites:

1. Execute the WebCenter Portal Installer a second time for each shared ORACLE_HOME, selecting an Installation Type of WebCenter Portal SOA Composites.
2. Verify that the WebCenter Portal composite archive has been installed.

Starting the Oracle WebCenter Portal Installer on WCPHOST1

## 16.3.1 Starting the Oracle WebCenter Portal Installer on WCPHOST1

To start the installation program:

1. Log in to WCPHOST1.
2. Go to the directory where you downloaded the installation program.
3. Launch the installation program by invoking the `java` executable from the JDK directory on your system, as shown in the example below.

   ```
   JAVA_HOME/bin/java -d64 -jar fmw_12.2.1.0.0_wcportal_generic.jar
   ```

   Be sure to replace the JDK location in these examples with the actual JDK location on your system.

   For information about downloading the software and locating the actual installer file name for your product, see Identifying and Obtaining Software Downloads for an Enterprise Deployment.

When the installation program appears, you are ready to begin the installation.

## 16.3.2 Navigating the Installation Screens

The installation program displays a series of screens, in the order listed in the following table.

If you need additional help with any of the installation screens, click the screen name.

| Screen | Description |
|---|---|
| Welcome | This screen introduces you to the product installer. |
| Auto Updates | Use this screen to automatically search My Oracle Support for available patches or automatically search a local directory for patches that you've already downloaded for your organization. |
| Installation Location | Use this screen to specify the location of your Oracle home directory.<br>For more information about Oracle Fusion Middleware directory structure, see "Selecting Directories for Installation and Configuration" in *Planning an Installation of Oracle Fusion Middleware*. |
| Installation Type | Use this screen to select the type of installation and consequently, the products and feature sets you want to install.<br>To install the SOA Composites for WebCenter Portal, select:<br>• **WebCenter Portal SOA Composites** |

| Screen | Description |
|---|---|
| Prerequisite Checks | This screen verifies that your system meets the minimum necessary requirements.<br>If there are any warning or error messages, you can refer to one of the following documents in the Roadmap for Verifying Your System Environment section in *Planning Your Oracle Fusion Middleware Infrastructure Installation*. |
| Installation Summary | Use this screen to verify the installation options you selected.<br>Click **Install** to begin the installation. |
| Installation Progress | This screen allows you to see the progress of the installation.<br>Click **Next** when the progress bar reaches 100% complete. |
| Installation Complete | Review the information on this screen, then click **Finish** to dismiss the installer. |

### 16.3.3 Verifying the Installed Files

Once the installation has been completed, verify that the WebCenter Portal SOA Composite and worklist details application archives have been written to the correct directory structure within ORACLE_HOME as follows:

```
ls ORACLE_HOME/wcportal/common/soa-composiste/wcp/sca_CommunityWorkflows.jar
ls ORACLE_HOME/wcportal/webcenter/applications/WebCenterWorklistDetailApp.ear
```

**Note:** The 12.2.1.0.0 General Availability release has a typo in the deployed path. Verify the directory path and file name carefully.

### 16.3.4 Performing the Installation on WCPHOST2

The installation should be repeated once for each shared file system containing a unique *ORACLE_HOME*. See Summary of the Shared Storage Volumes in an Enterprise Deployment.

## 16.4 Extending the Domain to Deploy the WebCenter Portal Workflows

WebCenter Portal workflows are deployed to Oracle SOA Server. To prepare the SOA cluster for workflows, you must extend the domain in which Oracle SOA is installed by using the template `oracle.wc_composite_template.jar`.

To extend the domain:

1. Run the following command to start the configuration wizard.

   ```
   ORACLE_HOME/oracle_common/common/bin/config.sh
   ```

2. On the Configuration Type screen, select **Update an existing domain**.

   In the **Domain Location** field, select the value of the ASERVER_HOME variable, which represents the complete path to the Administration Server domain home

you created in Creating the Initial Infrastructure Domain for an Enterprise Deployment.

`/u01/oracle/config/domains/domain_name/`

3. On the Templates screen, select the template in either of the following ways:

   - Select Update Domain Using Product Templates, then select:

     Oracle WebCenter Portal Composites - 12.2.1.0 [wcportal]

   - Select Update Domain Using Custom Template, and specify the following path in the Template location field:

     *ORACLE_HOME*`/wcportal/common/templates/wls/oracle.wc_composite_template.jar`

   The `oracle.wc_composite_template.jar` template automatically deploys:

   - `WebCenterWorklistDetailApp.ear`, the ADF application that displays invitations and messages.
   - `sca_CommunityWorkflows.jar`, the BPEL composite that manages the WebCenter Portal membership mechanism.

4. Review and continue through the remaining screens , until you reach page 7 of 10, Advanced Configuration. Select **Deployments and Services** and click **Next**.

5. Deployments Targeting.

   With the Oracle Web Services Manager Policy Manager deployed to a separate cluster, the default targeting of the WSM-PM application to the Portal, Collaboration, Portlet, In-Bound Refinery, Content, and SOA clusters should be removed.

   For each of the `Portal_Cluster`, `Collab_Cluster`, `Portlet_Cluster`, `IBR_Cluster`, `WCC_Cluster`, and `SOA_Cluster` in the Targets panel, select the wsm-pm application entry within the Application folder and click the left arrow button to remove it from the targets list.

6. Services Targeting.

   With the Oracle Web Services Manager Policy Manager deployed to a separate cluster, the default targeting of the WSM-PM service resources to the Portal, Collaboration, Portlet, In-Bound Refinery, Content, and SOA clusters should be removed.

   For each of the `Portal_Cluster`, `Collab_Cluster`, `Portlet_Cluster`, `IBR_Cluster`, `WCC_Cluster`, and `SOA_Cluster` in the Targets panel, select and remove the following resources from the targets list:

   - mds-owsm
   - WSM Startup Class

7. Reviewing Your Configuration Specifications and Configuring the Domain.

   The Configuration Summary screen contains the detailed configuration information for the domain you are about to create. Review the details of each item on the screen and verify that the information is correct.

You can go back to any of the previous screen if you need to make any changes, either by selecting **Back** or by selecting the required screen in the navigation pane.

**Note:** The Domain extension will not begin until you click **Update**.

## 16.5 Propagating the Extended Domain to the Domain Directories and Machines

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, complete the following steps:

1. Create a copy of the Managed Server domain directory and the Managed Server `applications` directory.
2. Run the following `pack` command on WCPHOST1 to create a template pack:

```
cd ORACLE_COMMON_HOME/common/bin

./pack.sh -managed=true
          -domain=ASERVER_HOME
          -template=/full_path/wcpdomaintemplateExtComposites.jar
          -template_name=wcp_domain_template_extension_composites
```

   In this example:

   - Replace *ASERVER_HOME* with the actual path to the domain directory you created on the shared storage device.
   - Replace *full_path* with the complete path to the location where you want to create the domain template jar file. You will need to reference this location when you copy or unpack the domain template jar file. It is recommended to choose a shared volume other than *ORACLE_HOME*, or write to `/tmp/` and copy the files manually between servers.

     You must specify a full path for the template jar file as part of the `-template` argument to the pack command:

     ```
     SHARED_CONFIG_DIR/domains/template_filename.jar
     ```

   - `wcpdomaintemplateExtComposites.jar` is a sample name for the JAR file you are creating, which will contain the domain configuration files, including the configuration files for the Oracle HTTP Server instances.
   - `wcp_domain_template_extension_composites` is the name assigned to the domain template file.

3. Run the following `unpack` command on WCPHOST1 to propagate the template created in the preceding step to the *MSERVER_HOME* directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME
            -template=/full_path/wcpdomaintemplateExtComposites.jar
            -app_dir=APPLICATION_HOME
            -overwrite_domain=true
```

   In this example:

- Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
- `wcpdomaintemplateExtComposites.jar` is the directory path and name of the template you created when you ran the pack command to pack up the domain on the shared storage device.
- The `-overwrite_domain=true` argument is necessary when you are 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.
- Replace *`APPLICATION_HOME`* with the complete path to the Application directory for the domain on local storage.

  **Tip:**

  For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

4. Run the following command on WCPHOST1 to copy the template pack created in step 1 to WCPHOST2, WCCHOST1, and WCCHOST2:

```
scp /full_path/wcpdomaintemplateExtComposites.jar oracle@WCPHOST2:/full_path/
scp /full_path/wcpdomaintemplateExtComposites.jar oracle@WCCHOST1:/full_path/
scp /full_path/wcpdomaintemplateExtComposites.jar oracle@WCCHOST2:/full_path/
```

5. Run the following `unpack` command on each of the remote hosts to deploy the domain template copied in the preceding step to the *MSERVER_HOME* directory:

```
cd ORACLE_COMMON_HOME/common/bin

./unpack.sh -domain=MSERVER_HOME
            -template=/full_path/wcpdomaintemplateExtComposites.jar
            -app_dir=APPLICATION_HOME
            -overwrite_domain=true
```

   In this example:

   - Replace *MSERVER_HOME* with the complete path to the domain home to be created on the local storage disk. This is the location where the copy of the domain will be unpacked.
   - `wcpdomaintemplateExtComposites.jar`is the directory path and name of the template you created when you ran the pack command to pack up the domain on the shared storage device.
   - The `-overwrite_domain=true` argument is necessary when you are 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.

- Replace *APPLICATION_HOME* with the complete path to the Application directory for the domain on local storage.

**Tip:**

For more information about the pack and unpack commands, see "Overview of the Pack and Unpack Commands" in *Creating Templates and Domains Using the Pack and Unpack Commands*.

## 16.6 Restoring customizations to setDomainEnv.sh after Unpacking the Domain

If any customizations have been made earlier to the `setDomainEnv.sh` files in *ASERVER_HOME* and *MSERVER_HOME*, then these customizations will need to be repeated after any domain extension.

Verify that all customizations have been restored before starting NodeManager or WebLogic Server instances.

On WCPHOST1:

1. Verify and update *ASERVER_HOME*`/bin/setDomainEnv.sh`.
2. Verify and update *MSERVER_HOME*`/bin/setDomainEnv.sh`.
3. Copy *MSERVER_HOME*`/bin/setDomainEnv.sh` to the other hosts (e.g. WCPHOST2, WCCHOST1, WCCHOST2).

**Note:** There are unique differences in parameter values stored in the `ASERVER_HOME` and `MSERVER_HOME` `setDomainEnv.sh` configuration files. The same file cannot be copied into both locations and should be edited separately. *MSERVER_HOME*`/bin/setDomainEnv.sh` can be copied across the environment consistently.

## 16.7 Updating the NodeManager Configuration After Unpacking the Domain

When extending a domain after setting up custom keystores, certificates, and custom identity aliases, the `nodemanager.properties` file in *MSERVER_HOME* may be overwritten with some values from the `nodemanager.properties` file for *ASERVER_HOME*. Specifically, the `ListenAddress` and/or `CustomIdentityAlias` values can be reset.

**Notes::**

- The `ListenAddress` may typically get reset on the *MSERVER_HOME* nodemanager residing on the same host as the *ASERVER_HOME* nodemanager. In this topology, WCCHOST1.
- In the previous chapters, prior to Enabling SSL Communication Between the SOA Servers and the Hardware Load Balancer, steps 2 through 4 regarding the `CustomIdentityAlias` may not be applicable.

For the *MSERVER_HOME*`/nodemanager/nodemanager.properties` file on each host:

1. Verify the correct `ListenAddress` parameter value and reset it, if required.

   ```
   grep ListenAddress MSERVER_HOME/nodemanager/nodemanager.properties
   ```

2. Confirm the list of configured Identity Aliases from the domain configuration file as a reference for the next command.

   ```
   grep server-private-key-alias ASERVER_HOME/config/config.xml | sort | uniq
   ```

3. Verify the current `CustomIdentityAlias` parameter value.

   ```
   grep CustomIdentityAlias MSERVER_HOME/nodemanager/nodemanager.properties
   ```

4. Reset the `CustomIdentityAlias` parameter value to the correct alias string appropriate for the current host, if required.

5. Restart the `nodemanager` process:

   ```
   kill `ps -eaf | grep weblogic.NodeManager | grep MSERVER_HOME | grep -v grep |
   awk '{print $2}' `
   nohup MSERVER_HOME/bin/startNodeManager.sh > MSERVER_HOME/nodemanager/
   nodemanager.out 2>&1 &
   ```

For more information, see Configuring Node Manager to Use the Custom Keystores.

# 16.8 Starting the Domain and Validating the WebCenter Portal SOA Composite Domain Extension

Start the entire domain and use Enterprise Manager to verify the deployment of the Portal SOA Composites and WebCenter Worklist Detail application.

Starting the Administration Server Using the Node Manager
: After you have configured the domain and configured the Node Manager, you can start the Administration Server, using the Node Manager. In an enterprise Deployment, the Node Manager is used to start and stop the Administration Server and all the Managed Servers in the domain.

Starting all Managed Servers
: Start all managed servers in the domain using the Weblogic Server Console, Enterprise Manager, or WLST.

Verifying the WebCenter Portal SOA Composites Deployment

## 16.8.1 Starting the Administration Server Using the Node Manager

After you have configured the domain and configured the Node Manager, you can start the Administration Server, using the Node Manager. In an enterprise Deployment, the Node Manager is used to start and stop the Administration Server and all the Managed Servers in the domain.

To start the Administration Server using the Node Manager:

1. Start the WebLogic Scripting Tool (WLST):

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

2. Connect to Node Manager using the Node Manager credentials:

```
wls:/offline>nmConnect('nodemanager_username','nodemanager_password',
            'ADMINVHN','5556','domain_name',
            'ASERVER_HOME')
```

**Note:**

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

*ASERVER_HOME*`/config/nodemanager`

3. Start the Administration Server:

```
nmStart('AdminServer')
```

**Note:**

When you start the Administration Server, it attempts to connect to Oracle Web Services Manager for WebServices policies. It is expected that, since the WSM-PM Managed Servers are not yet started, the following message will appear in the Administration Server log:

```
<Warning><oracle.wsm.resources.policymanager>
<WSM-02141><Unable to connect to the policy access service due to Oracle WSM
policy manager host server being down.>
```

4. Exit WLST:

```
exit()
```

## 16.8.2 Starting all Managed Servers

Start all managed servers in the domain using the Weblogic Server Console, Enterprise Manager, or WLST.

To assure all service dependencies are handled correctly as the applications come online, the recommended order is:

1. WSM-PM_Cluster
2. SOA_Cluster
3. IBR_Servers, Portlet_Cluster, Collab_Cluster
4. WCC_Cluster
5. Portal_Cluster

## 16.8.3 Verifying the WebCenter Portal SOA Composites Deployment

Two deployments are added when the domain is extended with the WebCenter Portal SOA Composites. These include one enterprise application archive and one SOA composites archive. These resources must be successfully deployed and validated before continuing with this domain extension. The SOA composites rely on the

application for the human tasks included in the workflows. They are deployed separately, using different processes.

- `WebCenterWorklistDetailApp.ear` — A standard Java EE web application located in *`ORACLE_HOME`*`/wcportal/webcenter/applications`
- `sca_CommunityWorkflows.jar` — A SOA Composite located in *`ORACLE_HOME`*`/wcportal/common/soa-composiste/wcp`

This section contains instructions for both the validation and deployment processes.

Confirming the WebCenter Portal SOA Composite and Application Deployments

Deploying the WebCenterWorklistDetailApp Application to the SOA_Cluster

Deploying the CommunityWorkflows SOA Composite to the SOA service

### 16.8.3.1 Confirming the WebCenter Portal SOA Composite and Application Deployments

To validate the `WebCenterWorklistDetailApp.ear` application deployment:

1. Connect to Enterprise Manager as the `weblogic_wcp` administrative user.
2. Verify that the `WebCenterWorklistDetailApp` application is listed **Target Navigation** > **Application Deployments**. If the application link is not listed, see section Deploying the WebCenterWorklistDetailApp Application to the SOA_Cluster.
3. If the `WebCenterWorklistDetailApp` application is listed, click on the link and validate that the State is listed as **Active** and the Health is **OK** in the Summary view. Also, validate that the **SOA_Cluster** is listed in the Targets column of the Deployments view.

   If the `WebCenterWorklistDetailApp` does not show the SOA_Cluster in the Targets column, complete the following steps:

   a. From the Domain Application Deployment drop-down list, select **Administration** > **Targets**.
   b. From the lock icon in the upper-right corner, select **Lock & Edit**.
   c. Select **WebCenterWorklistDetailApp EAR**, then click **Change Targets**.
   d. In the pop-up window, select **SOA_Cluster** and then select the **All configured Servers in this cluster** option.
   e. Click **OK**. After the changes are complete a confirmation message is displayed.
   f. From the lock icon in the upper-right corner, select **Activate Changes**.
   g. Restart the managed servers in the SOA_Cluster.
4. Expand the **Target Navigation** panel and navigate to the **WebLogic Domain** > **domain-name** > **SOA_Cluster**.
5. From the WebLogic Cluster drop-down menu, select **Deployments**.

6. Verify that the `WebCenterWorklistDetailApp` is listed with a green *up* arrow status and a state of **Active**.

   If the `WebCenterWorklistDetailApp` is not deployed to the SOA_Cluster, perform the deployment after all validation steps are completed. See Deploying the WebCenterWorklistDetailApp Application to the SOA_Cluster.

To validate the `sca_CommunityWorkflows.jar` SOA composites deployment:

1. Expand the **Target Navigation** panel and navigate to the **SOA** > **soa-infra (WLS_SOA1)** service
2. Click the **Deployed Composites** tab.
3. Verify that the CommunitWorkflows [12.2.1.0.0] composite is listed with a green *up* arrow for status.

   If the CommunityWorkflows composite is not deployed to the SOA service, perform the deployment after all validation steps are completed. See Deploying the CommunityWorkflows SOA Composite to the SOA service.

#### 16.8.3.2 Deploying the WebCenterWorklistDetailApp Application to the SOA_Cluster

If the `WebCenterWorklistDetailApp` application needs to be deployed, perform the following steps:

1. Connect to Enterprise Manager as the weblogic_wcp administrative user .
2. Expand the **Target Navigation** panel and navigate to the **WebLogic Domain** > ***domain-name*** > **SOA_Cluster**
3. From the WebLogic Cluster drop-down menu, select **Deployments**.
4. Verify that the `WebCenterWorklistDetailApp` is not listed.
5. From the Deployment drop-down menu, select **Deploy**.
6. Select an appropriate deployment scope. For out-of-box configurations, the appropriate scope is **global**.
7. Select **Archive on the server where Enterprise Manager is running**.
8. Enter: *`ORACLE_HOME`*`/wcportal/webcenter/applications/WebCenterWorklistDetailApp.ear`.
9. Select **Create a new deployment plan when deployment configuration is done** .
10. Select **Deploy this archive or exploded directory as an application**.
11. Click **Next**.
12. On the Select Target view, make sure that only the **SOA_Cluster** is checked and the **All configured Servers** in this cluster option is selected.
13. On the Application Attributes view, change only the distribution option to: **Install and start application (servicing all requests)**. Do not alter any other application attributes
14. Click **Deploy**. The remaining application deployment configurations do not need to be modified.

15. Observe the progress messages provided in the **Processing: Deploy** modal dialog box that appears and wait for it to complete.
16. Observe that the dialog box is updated with a *Deployment Succeeded* message.
17. Close the dialog box.
18. Verify that the new application deployment is listed with a green *up* arrow status and a state of **Active**.

See Deploying Java EE Applications Using Fusion Middleware Control in *Administering Oracle Fusion Middleware* for details on how to deploy the enterprise application archive.

#### 16.8.3.3 Deploying the CommunityWorkflows SOA Composite to the SOA service

If the `CommunityWorkflows SOA` composite needs to be deployed, perform the following steps:

1. Connect to Enterprise Manager as the weblogic_wcp administrative user .
2. Expand the **Target Navigation** panel and navigate to the **SOA** > **soa-infra (WLS_SOA1)** service.
3. Click on the **Deployed Composites** tab.
4. Verify the CommunityWorkflows composite is listed as *Up* and *Active*. If not listed, or the list says *No Composites Found*, then continue with these deployment steps. If status is down, select and start the CommunityWorkflows composite.
5. Click **Deploy**.
6. Select **Archive on the server where Enterprise Manager is running**.
7. Enter: *`ORACLE_HOME`*`/wcportal/common/soa-composite/wcp/sca_CommunityWorkflows.jar`
8. Select **No external configuration plan is required**.
9. Click **Next**.
10. Confirm the deployment target is **/Domain_< domain_name >/< domain_name >/SOA_Cluster**
11. Confirm the appropriate SOA Partition. For out-of-box configurations, the appropriate partition is **default**.
12. Click **Next**.
13. Confirm the **Deploy as default revision** selection as this is the first time the composites are getting deployed.
14. Enter the administrative identity and credential again for this session: User Name and Password for `weblogic_wcp`.
15. Click **Deploy**.
16. Observe the progress messages provided in the **Processing: Deploy** modal dialog box that appears and wait for it to complete.

17. Observe that the dialog box is updated with a **Deployment Succeeded** message.
18. Close the dialog box.
19. Observe that Enterprise Manager now displays the `CommunityWorkflows[12.2.1.0.0]` SOA composite dashboard view with several components and services.

See Deploying SOA Composite Applications in *Administering Oracle SOA Suite and Oracle Business Process Management Suite* for details on how to deploy the composite.

## 16.9 Configuring WS-Security for Oracle SOA and WebCenter Portal

WebCenter Portal Web services, deployed to Oracle WebCenter Portal, facilitate communication between WebCenter Portal and the SOA server. You must secure these Web service calls.

---

**Note:** Some of the key aliases and other properties values used in this configuration are specifically required by the deployed products. This process has been tuned specifically for a combined topology with Oracle SOA and WebCenter Portal in the same domain. Customizing this process beyond the provided instructions is not recommended.

For more information on configuration for a two-domain topology, see Oracle SOA and WebCenter Portal - WS-Security Configuration in *Installing and Configuring Oracle WebCenter Portal*.

---

Set up WS-Security by creating a security application stripe and keystore for WebCenter Portal and the SOA Suite BPEL Server to use. Oracle Fusion Middleware 12c implements these keystores using the Keystore Security Service (KSS) configured via Enterprise Manager or WLST commands.

For more information, see Configuring Keystores for Message Protection in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

For syntax and reference information about the KSS commands, see OPSS Keystore Service Commands in *Oracle Fusion Middleware Infrastructure Security WLST Command Reference*.

Creating the WebCenter Portal Keystore via WLST

### 16.9.1 Creating the WebCenter Portal Keystore via WLST

After you create the Oracle Web Services Manager keystore, create a new WebCenter Portal keystore.

1. Start WLST and connect to the Administration Server as the administrative LDAP user.

```
ORACLE_COMMON_HOME/common/bin/wlst.sh
connect("weblogic_wcp", "weblogic_admin_pwd", "t3://ADMINVHN:7001")
```

2. Use the following WLST command to get an OPSS service command object:

```
svc = getOpssService(name='KeyStoreService')
```

3. Create the keystore using the following WLST command:

```
svc.createKeyStore(appStripe='WCPortalStripe', name='producer',
password='password', permission=true)
```

Where:

- *appstripe* — The keystore stripe name. Keys and certificates created in the keystore reside in an application stripe or product, and each stripe in a domain is uniquely named
- *keystore_name* — The name of the keystore you are creating; typically, you use a name to help identify the component or endpoint being secured
- *password* — Enter the password you want to use for this keystore.
- *permission* — false if protected by both permission and password (true if keystore is protected by permission only)

4. Generate the key pair for this newly created keystore, supplying an appropriate password and setting the domain name, organization, location(city), state, and country appropriately:

```
svc.generateKeyPair(appStripe='WCPortalStripe' , name='producer',
password='password', alias='producer', keypassword='password', dn='CN=Producer,
OU=Producer, O=MyOrganization, L=MyTown, ST=MyState, C=US', keysize='2048')
```

Where:

- *appstripe* — The keystore stripe name. Keys and certificates created in the keystore reside in an application stripe or product, and each stripe in a domain is uniquely named
- *keystore_name* — The name of the keystore you are creating; typically, you use a name to help identify the component or endpoint being secured
- *password* — The password you defined when you created the keystore.
- *dn* — Distinguished Name; used to uniquely identify and organize the key pair within a hierarchical naming structure. Update the `OU`=*domain_name*, `O`=*MyOrg*, `L`=*MyTown*, `ST`=*MyState*, `C`=*US*, portions of the DN to match your environment and organization appropriately.
- *keysize* - number of bits for the encryption key, should be at least 2048
- *alias* — Public Key Alias
- *keypassword* — Enter a password for new public key that you are creating.

5. Export the producer certificate (which will be used by the consumer):

```
svc.exportKeyStoreCertificate(appStripe='WCPortalStripe', name='producer',
password='password', alias='producer',
type='TrustedCertificate',filepath='KEYSTORE_HOME/ksscert_wcportalproducer.crt')
```

Where:

- *appstripe* — The keystore stripe name. Keys and certificates created in the keystore reside in an application stripe or product, and each stripe in a domain is uniquely named
- *name* — Keystore name

- *password* — Keystore password
- *alias* — Public Key Alias
- *keypassword* — Password for new public key
- *filepath* — Certificate path

6. Import the certificate exported by the producer for use by the consumer web service:

```
svc.importKeyStoreCertificate(appStripe='WCPortalStripe', name='producer',
password='password', alias='webcenter_spaces_ws', keypassword='keypassword',
type='TrustedCertificate', filepath='KEYSTORE_HOME/ksscert_wcportalproducer.crt')
```

Where:

- *password* — Keystore password
- *keypassword* — Password for new public key
- *filepath* — Certificate path

---

**Note:**

The alias for the `importKeyStoreCertificate` command must always be set to `webcenter_spaces_ws`. Do not attempt to change this alias; otherwise, the web services communications will fail. This alias is used in the default configuration of the Web services policy security.

---

7. Register the producer stripe:

```
configureWSMKeystore('/WLS/domain_name','KSS', 'kss://WCPortalStripe/producer',
signAlias='producer', cryptAlias='producer', signAliasPassword='password',
cryptAliasPassword='password')
```

Where:

- *domain_name* – The name of the WebCenter Portal domain; the "/WLS/" prefix is required to provide context for the Web Services Manager manager
- KSS — The keystore type
- `kss://WCPortalStripe/producer`— The location of the keystore: keys and certificates created in the keystore reside in an application stripe or product, and each stripe in a domain is uniquely named
- *signAlias* – The alias of the signature key; the value must match the value in the keystore, in this case, 'producer'
- *cryptAlias* — The alias of the encryption key. The value that you specify here must match the value in the keystore, in this case, 'producer'
- *signAliasPassword*— The password for the certificate specified for the *signAlias* as configured earlier
- *cryptAliasPassword*— The password for the certificate specified for the *cryptAlias* as configured earlier

**Note:** When using a KSS keystore type, the `configureWSMKeystore()` command may issue warnings that the passwords are not required. In this specific case, when services are using policies that mandate message protection, the passwords are required, otherwise the services cannot use the certificates to encrypt and decrypt appropriately. Be sure to include the password parameters as indicated in the example.

For more information, see "Configuring the OWSM Keystore Using WLST" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

8. Grant Keystore Permission for the newly created `producer` keystore in the WCPortalStripe stripe:

```
grantPermission(permClass="oracle.security.jps.service.keystore.KeyStoreAccessPerm
ission", permTarget="stripeName=WCPortalStripe,keystoreName=producer,alias=*",
permActions="read")
```

**Note:**

The `StripeName` and `keystoreName` values in the `permTarget` value must match values used in earlier steps. No other changes are required to this command.

## 16.10 Verifying Application Roles

Before you configure WebCenter Portal with SOA Suite, understand and verify the `SOAAdmin` and `BPMWorkflowAdmin` application roles.

The memberships of the SOAAdmin and BPMWorkflowAdmin application roles can be listed as follows:

```
ORACLE_COMMON_HOME/common/bin/wlst.sh
connect('weblogic_wcp','password', 't3://ADMINVHN:7001')
listAppRoleMembers(appStripe="soa-infra", appRoleName="SOAAdmin")
listAppRoleMembers(appStripe="soa-infra", appRoleName="BPMWorkflowAdmin")
```

To revoke a user or group membership from an application role, consider following WLST examples:

```
revokeAppRole(appStripe="soa-infra", appRoleName="BPMWorkflowAdmin",
principalClass="weblogic.security.principal.WLSUserImpl", principalName="weblogic")
revokeAppRole(appStripe="soa-infra", appRoleName="BPMWorkflowAdmin",
principalClass="weblogic.security.principal.WLSGroupImpl",
principalName="Administrators")
```

To specifically grant a user membership to an application role, follow this example:

```
grantAppRole(appStripe="soa-infra", appRoleName="BPMWorkflowAdmin",
principalClass="weblogic.security.principal.WLSUserImpl",
principalName="weblogic_wcp")
```

For the LDAP group configurations in the enterprise deployment environment, it is not necessary to grant the `weblogic_wcp` user specific access. The `WCPAdministrators` group should already be part of the `SOAAdmin` application role and inherit membership to the `BPMWorkflowAdmin` application role.

For more information about configuring a remote LDAP server for the enterprise deployment, see Creating a New LDAP Authenticator and Provisioning Enterprise Deployment Users and Group.

For more information about SOA application role configurations, see Configuring Roles for Administration of an Enterprise Deployment.

## 16.11 Creating the Connection to the BPEL Server

WebCenter Portal uses BPEL server to host internal workflows, such as worklists, membership notifications, subscription requests, and so on. BPEL Services are configured on the SOA Managed Servers. To enable workflow functionality for WebCenter Portal, a connection to the BPEL service is required.

---

**Note:**

WebCenter Portal workflows must be deployed on the SOA managed server that WebCenter Portal is configured to use. See also, Back-End Requirements for WebCenter Portal Workflows in *Installing and Configuring Oracle WebCenter Portal*.

---

To configure a connection for worklist notifications:

1. Log in to Fusion Middleware Control, and navigate to the home page for WebCenter Portal.

   See "Navigating to the Home Page for WebCenter Portal" in *Administering Oracle WebCenter Portal*.

2. From the **WebCenter Portal** menu, select **Settings**, then **Application Configuration** .

3. In the BPEL SOAP URL field, specify the internal load-balanced URL.

   For example:

   ```
   http://wcp-internal.example.com:80
   ```

4. In the Link URL field, specify the public front-end load-balanced URL for the environment.

   For example:

   ```
   https://wcp.example.com:443
   ```

5. Select **Enable WebCenter Portal Workflows**.

6. Click **Apply**.

7. Restart the Portal_Cluster for this change to take effect.

   See "Starting and Stopping Managed Servers for WebCenter Portal Application Deployments" in *Administering Oracle WebCenter Portal*.

## 16.12 Validating the Connection to the BPEL Server

After you create the connection to the BPEL Server, validate the connection to be sure it is working properly.

Use the WLST command `listWorklistConnections` to display the configured connections and validate the connection details.

For example:

```
listWorklistConnections(appName='webcenter', server='WC_Portal1')
```

Use the listed URL property value to construct a valid worklist application URL and validate access using a browser. Append the listed URL property value with the path `/integration/worklistapp`, to generate an appropriate URL for testing.

## 16.13 Configuring WebCenter Portal Workflow Notifications to be Sent by Email

WebCenter Portal can use human workflows (requiring human interaction), which are integrated with SOA workflows. The SOA server can configure email so that notifications are delivered to a user's inbox, where the user can accept or reject the notification.

This topic briefly explains how to enable email notifications and set your mail server details to have WebCenter Portal workflow notifications sent through email. Both outbound and incoming email addresses or mailboxes that are dedicated to portal workflow notification and reply processing are needed for full functionality. For a more detailed description, see Configuring Human Workflow Notification Properties in *Administering Oracle SOA Suite and Oracle Business Process Management Suite*.

1. Connect to Enterprise Manager Fusion Middleware Control as the `weblogic_wcp` administrative user.
2. Expand the Target Navigation panel and navigate to the **SOA** > **soa-infra (WLS_SOA1) service**.
3. From the **SOA Infrastructure** drop-down menu, select **SOA Administration** > **Workflow Properties**.
4. Set the Notification Mode to: **Email**
5. Provide the correct email addresses for the Notification Service.
6. Click **Apply** and then confirm when prompted. Verify the returned message that confirms changes have been applied.
7. Click the **Go to the Messaging Driver page** link.
8. In the Associated Drivers section, Click the **Configure Driver** icon for the **User Messaging Email Driver**.
9. Click **Create** to configure an email driver, if one does not already exist.

   For instructions on how to configure the email driver for notifications, see Configuring an Email Driver for Notifications in *Using Oracle Managed File Transfer*.
10. Once all required email driver configurations are completed, click **Test** and validate successful test status.
11. Click **Apply** to save the email driver configuration.
12. Verify that the new UMS driver configuration shows up in the **Email Driver Properties table** view.

13. Restart the SOA Cluster. No configuration or restart is required for WebCenter Portal.

## 16.14 Testing the Oracle BPM Worklist Application in WebCenter Portal

Testing of the WebCenter Portal invitation and membership workflows and email notifications can be performed using end-user accounts and requires specific portal run-time configuration to set up the test case.

See Task 7 in the Configuration Roadmap for WebCenter Portal Workflows section in the *Administering Oracle WebCenter Portal Guide* for more information.

# Part IV

# Common Configuration and Management Procedures for an Enterprise Deployment

The following topics contain configuration and management procedures that are required or recommended for a typical enterprise deployment.

# 17

# Common Configuration and Management Tasks for an Enterprise Deployment

The following topics describe configuration and management tasks you will likely need to perform on the enterprise deployment environment.

Verifying Manual Failover of the Administration Server
: In case a host computer fails, you can fail over the Administration Server to another host. The following sections provide the steps to verify the failover and failback of the Administration Server from WCPHOST1 and WCPHOST2.

Enabling SSL Communication Between the Middle Tier and the Hardware Load Balancer
: This section describes how to enable SSL communication between the middle tier and the hardware load balancer.

Configuring Roles for Administration of an Enterprise Deployment
: This section provides a summary of products with specific administration roles and provides instructions to add a product-specific administration role to the Enterprise Deployment Administration group.

Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment
: The following topics provide guidelines for when to use JDBC persistent stores for transaction logs (TLOGs) and JMS. They also provide the procedures you can use to configure the persistent stores in a supported database.

Performing Backups and Recoveries for an Enterprise Deployment
: This section provides guidelines for making sure you back up the necessary directories and configuration data for an Oracle WebCenter Portal enterprise deployment.

## 17.1 Verifying Manual Failover of the Administration Server

In case a host computer fails, you can fail over the Administration Server to another host. The following sections provide the steps to verify the failover and failback of the Administration Server from WCPHOST1 and WCPHOST2.

Assumptions:

- The Administration Server is configured to listen on ADMINVHN, and not on localhost or ANY address.

  For more information about the ADMINVHN virtual IP address, see Reserving the Required IP Addresses for an Enterprise Deployment.

- These procedures assume that the Administration Server domain home (ASERVER_HOME) has been mounted on both host computers. This ensures that

the Administration Server domain configuration files and the persistent stores are saved on the shared storage device.

- The Administration Server is failed over from WCPHOST1 to WCPHOST2, and the two nodes have these IPs:
  - WCPHOST1: 100.200.140.165
  - WCPHOST2: 100.200.140.205
  - ADMINVHN : 100.200.140.206. This is the Virtual IP where the Administration Server is running, assigned to ethX:Y, available in WCPHOST1 and WCPHOST2.
- Oracle WebLogic Server and Oracle Fusion Middleware components have been installed in WCPHOST2 as described in the specific configuration chapters in this guide.

  Specifically, both host computers use the exact same path to reference the binary files in the Oracle home.

The following topics provide details on how to perform a test of the Administration Server failover procedure.

Failing Over the Administration Server to a Different Host
: The following procedure shows how to fail over the Administration Server to a different node (WCPHOST2). Note that even after failover, the Administration Server will still use the same Oracle WebLogic Server *machine* (which is a logical machine, not a physical machine).

Validating Access to the Administration Server on WCPHOST2 Through Oracle HTTP Server
: After you perform a manual failover of the Administration Server, it is important to verify that you can access the Administration Server, using the standard administration URLs.

Failing the Administration Server Back to WCPHOST1
: After you have tested a manual Administration Server failover, and after you have validated that you can access the administration URLs after the failover, you can then migrate the Administration Server back to its original host.

## 17.1.1 Failing Over the Administration Server to a Different Host

The following procedure shows how to fail over the Administration Server to a different node (WCPHOST2). Note that even after failover, the Administration Server will still use the same Oracle WebLogic Server *machine* (which is a logical machine, not a physical machine).

This procedure assumes you've configured a per domain Node Manager for the enterprise topology. For more information, see About the Node Manager Configuration in a Typical Enterprise Deployment

To fail over the Administration Server to a different host:

1. Stop the Administration Server.
2. Stop the Node Manager in the Administration Server domain directory (ASERVER_HOME).

3. Migrate the ADMINVHN virtual IP address to the second host:

   a. Run the following command as root on WCPHOST1(where X:Y is the current interface used by ADMINVHN):

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

   b. Run the following command as root on WCPHOST2:

      ```
      /sbin/ifconfig <interface:index> ADMINVHN netmask <netmask>
      ```

      **Note:** The index should be different than that of the BI Server 2 on the BIHOST2.

      For example:

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

      **Note:**

      Ensure that the netmask and interface to be used to match the available network configuration in WCPHOST2.

4. Update the routing tables using `arping`, for example:

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

5. Start the Node Manager in the Administration Server domain home on WCPHOST2.

6. Start the Administration Server on WCPHOST2.

7. Test that you can access the Administration Server on WCPHOST2 as follows:

   a. Ensure that you can access the Oracle WebLogic Server Administration Console using the following URL:

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

   b. Check that you can access and verify the status of components in Fusion Middleware Control using the following URL:

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

## 17.1.2 Validating Access to the Administration Server on WCPHOST2 Through Oracle HTTP Server

After you perform a manual failover of the Administration Server, it is important to verify that you can access the Administration Server, using the standard administration URLs.

From the load balancer, access the following URLs to ensure that you can access the Administration Server when it is running on WCPHOST2:

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

  This URL should display the WebLogic Server Administration console.

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

This URL should display Oracle Enterprise Manager Fusion Middleware Control.

### 17.1.3 Failing the Administration Server Back to WCPHOST1

After you have tested a manual Administration Server failover, and after you have validated that you can access the administration URLs after the failover, you can then migrate the Administration Server back to its original host.

1. Stop the Administration Server.
2. Stop the Node Manager in the Administration Server domain home on WCPHOST2.
3. Run the following command as root on WCPHOST2.

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

4. Run the following command as root on WCPHOST1:

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

   **Note:**

   Ensure that the netmask and interface to be used match the available network configuration in WCPHOST1

5. Update the routing tables using `arping` on WCPHOST1:

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

6. Start the Node Manager in the Administration Server domain home on WCPHOST1.
7. Start the Administration Server on WCPHOST1.
8. Test that you can access the Oracle WebLogic Server Administration Console using the following URL:

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

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

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

## 17.2 Enabling SSL Communication Between the Middle Tier and the Hardware Load Balancer

This section describes how to enable SSL communication between the middle tier and the hardware load balancer.

**Note:**

The following steps are applicable if the hardware load balancer is configured with SSL and the front end address of the system has been secured accordingly.



## 17.2.1 When is SSL Communication Between the Middle Tier and Load Balancer Necessary?

In an enterprise deployment, there are scenarios where the software running on the middle tier must access the front-end SSL address of the hardware load balancer. In these scenarios, an appropriate SSL handshake must take place between the load balancer and the invoking servers. This handshake is not possible unless the Administration Server and Managed Servers on the middle tier are started using the appropriate SSL configuration.

## 17.2.2 Generating Self-Signed Certificates Using the utils.CertGen Utility

This section describes the procedure for creating self-signed certificates on WCPHOST1. Create these certificates using the network name or alias of the host.

The directory where keystores and trust keystores are maintained must be on shared storage that is accessible from all nodes so that when the servers fail over (manually or with server migration), the appropriate certificates can be accessed from the failover node. Oracle recommends using central or shared stores for the certificates used for different purposes (for example, SSL set up for HTTP invocations).For more information, see the information on filesystem specifications for the KEYSTORE_HOME location provided in Understanding the Recommended Directory Structure for an Enterprise Deployment.

For information on using trust CA certificates instead, see the information about configuring identity and trust in *Oracle Fusion Middleware Securing Oracle WebLogic Server*.

### About Passwords

The passwords used in this guide are used only as examples. Use secure passwords in a production environment. For example, use passwords that include both uppercase and lowercase characters as well as numbers.

To create self-signed certificates:

1. Temporarily, set up your environment by running the following command: *WL_HOME*`/server/bin/setWLSEnv.sh` script:

   ```
   . WL_HOME/server/bin/setWLSEnv.sh
   ```

   Note that there is a dot(.) and space( ) preceding the script name in order to source the shell script in the current shell.

2. Verify that the CLASSPATH environment variable is set:

   ```
   echo $CLASSPATH
   ```

3. Verify that the shared configuration directory folder has been created and mounted to shared storage correctly as described in Preparing the File System for an Enterprise Deployment.

   For example, use the following command to verify that the shared configuration directory is available to each host:

   ```
   df -h | grep -B1 SHARED_CONFIG_DIR
   ```

   Replace *SHARED_CONFIG_DIR* with the actual path to your shared configuration directory.

   You can also do a listing of the directory to ensure it is available to the host:

   ```
   ls -al SHARED_CONFIG_DIR
   ```

4. Create the keystore home folder structure if does not already exist.

   For example:

   ```
   cd SHARED_CONFIG_DIR
   mkdir keystores
   chown oracle:oinstall keystores
   chmod 750 keystores
   export KEYSTORE_HOME=$SHARED_CONFIG_DIR/keystores
   ```

5. Change directory to the keystore home:

   ```
   cd KEYSTORE_HOME
   ```

6. Run the `utils.CertGen` tool to create the certificates for both the physical host names and the virtual host names used by servers in the node.

   Syntax:

   ```
   java utils.CertGen key_passphrase cert_file_name key_file_name [export |
   domestic] [hostname]
   ```

   Examples:

   ```
   java utils.CertGen password ADMINVHN.example.com_cert \
         ADMINVHN.example.com_key domestic ADMINVHN.example.com

   java utils.CertGen password WCPHOST1.example.com_cert \
         WCPHOST1.example.com_key domestic WCPHOST1.example.com
   ```

7. Repeat the above step for all the remaining hosts used in the system (for example, WCPHOST2).

### 17.2.3 Creating an Identity Keystore Using the utils.ImportPrivateKey Utility

This section describes how to create an Identity Keystore on WCPHOST1.example.com.

In previous sections you have created certificates and keys that reside on a shared storage. In this section, the certificate and private key for both WCPHOST1 and ADMINVHN are imported into a new Identity Store. Make sure that you use a different alias for each of the certificate/key pair imported.

---

**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.

---

1. Import the certificate and private key for ADMINVHN and WCPHOST1 into the Identity Store. Make sure that you use a different alias for each of the certificate/key pair imported.

   Syntax:

```
java utils.ImportPrivateKey
      -certfile cert_file
      -keyfile private_key_file
      [-keyfilepass private_key_password]
      -keystore keystore
      -storepass storepass
      [-storetype storetype]
      -alias alias
      [-keypass keypass]
```

   ---

   **Note:**

   Default keystore_type is `jks`.

   ---

   Examples:

```
java utils.ImportPrivateKey\
     -certfile KEYSTORE_HOME/ADMINVHN.example.com_cert.pem\
     -keyfile KEYSTORE_HOME/ADMINVHN.example.com_key.pem\
     -keyfilepass password\
     -keystore appIdentityKeyStore.jks\
     -storepass password\
     -alias ADMINVHN\
     -keypass password\

java utils.ImportPrivateKey\
     -certfile KEYSTORE_HOME/WCPHOST1.example.com_cert.pem\
     -keyfile KEYSTORE_HOME/WCPHOST1.example.com_key.pem\
     -keyfilepass password\
     -keystore appIdentityKeyStore.jks\
     -storepass password\
     -alias WCPHOST1\
     -keypass password\
```

2. Repeat the above step for all the remaining hosts used in the system (for example, WCPHOST2).

### 17.2.4 Creating a Trust Keystore Using the Keytool Utility

To create the Trust Keystore on WCPHOST1.example.com.

1. Copy the standard java keystore to create the new trust keystore since it already contains most of the root CA certificates needed.

   Oracle does not recommend modifying the standard Java trust key store directly. Copy the standard Java keystore CA certificates located under the WL_HOME/server/lib directory to the same directory as the certificates. For example:

   ```
   cp WL_HOME/server/lib/cacerts KEYSTORE_HOME/appTrustKeyStore.jks
   ```

2. Use the keytool utility to change the default password.

   The default password for the standard Java keystore is `changeit`. Oracle recommends always changing the default password, as follows:

   ```
   keytool -storepasswd -new NewPassword -keystore TrustKeyStore -storepass
   Original_Password
   ```

   For example:

   ```
   keytool -storepasswd -new password -keystore appTrustKeyStore.jks -storepass
   changeit
   ```

3. Import the CA certificate into the `appTrustKeyStore` using the keytool utility.

   The CA certificate `CertGenCA.der` is used to sign all certificates generated by the `utils.CertGen` tool and is located at *WL_HOME*`/server/lib` directory.

   Use the following syntax to import the certificate:

   ```
   keytool -import -v -noprompt -trustcacerts -alias AliasName -file CAFileLocation -
   keystore KeyStoreLocation -storepass KeyStore_Password
   ```

   For example:

   ```
   keytool -import -v -noprompt -trustcacerts -alias clientCACert -file WL_HOME/
   server/lib/CertGenCA.der -keystore appTrustKeyStore.jks -storepass password
   ```

### 17.2.5 Importing the Load Balancer Certificate into the Trust Store

For the SSL handshake to behave properly, the load balancer's certificate needs to be added to the WLS servers trust store. For adding it, follow these steps:

1. Access the site on SSL with a browser (this add the server's certificate to the browser's repository).

2. From the browser's certificate management tool, export the certificate to a file that is on the server's file system (with a file name like `wcp.example.com`).

3. Use the keytool to import the load balancer's certificate into the truststore:

   ```
   keytool -import -file wcp.example.com -v -keystore appTrustKeyStore.jks
   ```

### 17.2.6 Adding the Updated Trust Store to the Oracle WebLogic Server Start Scripts

The `setDomainEnv.sh` script is provided by Oracle WebLogic Server and is used to start the Administration Server and the Managed Servers in the domain. To ensure that each server accesses the updated trust store, edit the `setDomainEnv.sh` script in each of the domain home directories in the enterprise deployment.

1. Log in to WCCHOST1 and open the following file with a text editor:

   *ASERVER_HOME*`/bin/setDomainEnv.sh`

2. Replace reference to the existing `DemoTrustStore` entry with the following entry:

   **Note:**

   All the values for EXTRA_JAVA_PROPERTIES must be on one line in the file, followed by the export command on a new line.

```
EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES} -Dsoa.archives.dir=$
{SOA_ORACLE_HOME}/soa -Djavax.net.ssl.trustStore=/u01/oracle/certs/
appTrustKeyStore.jks"
export EXTRA_JAVA_PROPERTIES
```

3. Make the same change to the `setDomainEnv.sh` file in the *MSERVER_HOME*`/bin` directory WCCHOST1, WCCHOST2, WEBHOST1, and WEBHOST2.

   **Note:**

   The `setDomainEnv.sh` file cannot be copied between *ASERVER_HOME*`/bin` and *MSERVER_HOME*`/bin` as there are differences in the files for these two domain home locations. *MSERVER_HOME*`/bin/setDomainEnv.sh` can be copied between hosts.

   WebLogic Server will automatically overwrite the `setDomainEnv.sh` file after each domain extension. Some patches may also replace this file. Verify your customizations to `setDomainEnv.sh` after each of these types of maintenance operations.

### 17.2.7 Configuring Node Manager to Use the Custom Keystores

To configure the Node Manager to use the custom keystores, add the following lines to the end of the `nodemanager.properties` files located both in *ASERVER_HOME*`/nodemanager` and *MSERVER_HOME*`/nodemanager` directories in all nodes:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=Identity KeyStore
CustomIdentityKeyStorePassPhrase=Identity KeyStore Passwd
CustomIdentityAlias=Identity Key Store Alias
CustomIdentityPrivateKeyPassPhrase=Private Key used when creating Certificate
```

Make sure to use the correct value for `CustomIdentityAlias` for Node Manager's listen address. For example, in the WCPHOST1 *MSERVER_HOME*, use the alias WCPHOST1 and in the *ASERVER_HOME* on WCPHOST1, use the alias *ADMINVHN* according to the steps in Creating an Identity Keystore Using the utils.ImportPrivateKey Utility.

```
(appIdentity2 mapped to the WCPHOST1 listen address).
Example for Node 1:
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=KEYSTORE_HOME/appIdentityKeyStore.jks
CustomIdentityKeyStorePassPhrase=password
CustomIdentityAlias=appIdentity1
CustomIdentityPrivateKeyPassPhrase=password
```

The passphrase entries in the `nodemanager.properties` file are encrypted when you start Node Manager as described in "Starting the Node Manager on WCPHOST1." For security reasons, minimize the time the entries in the `nodemanager.properties` file are left unencrypted. After you edit the file, restart Node Manager as soon as possible so that the entries are encrypted.

---

**Note:** The `CustomIdentityAlias` value will need to be corrected every time the domain is extended after this configuration is performed. An unpack operation will replace the `CustomIdentityAlias` with the Administration Server's value when the domain configuration is written.

---

## 17.2.8 Configuring WebLogic Servers to Use the Custom Keystores

Configure the WebLogic Servers to use the custom keystores using the Oracle WebLogic Server Administration Console. Complete this procedure for the Administration Server and the Managed Servers that require access to the front end LBR on SSL.

To configure the identity and trust keystores:

1. Log in to the Administration Console, and click **Lock & Edit**.
2. In the left pane, expand **Environment**, and select **Servers**.
3. Click the name of the server for which you want to configure the identity and trust keystores.
4. Select **Configuration**, and then **Keystores**.
5. In the **Keystores** field, click **Change**, and select **Custom Identity and Custom Trust** method for storing and managing private keys/digital certificate pairs and trusted CA certificates, and click Save.
6. In the Identity section, define attributes for the identity keystore.
   - Custom Identity Keystore: Enter the fully qualified path to the identity keystore:

     `KEYSTORE_HOME/appIdentityKeyStore.jks`
   - Custom Identity Keystore Type: Leave this field blank, it defaults to JKS.
   - Custom Identity Keystore Passphrase: Enter the password Keystore_Password you provided in Creating an Identity Keystore Using the utils.ImportPrivateKey Utility

This attribute may be optional or required depending on the type of keystore. All keystores require the passphrase in order to write to the keystore. However, some keystores do not require the passphrase to read from the keystore. WebLogic Server reads only from the keystore, so whether or not you define this property depends on the requirements of the keystore.

7. In the Trust section, define properties for the trust keystore:
   - Custom Trust Keystore: Enter the fully qualified path to the trust keystore:

     *KEYSTORE_HOME*/appTrustKeyStore.jks

   - Custom Trust Keystore Type: Leave this field blank, it defaults to JKS.
   - Custom Trust Keystore Passphrase: The password you provided in as New_Password in "Creating a Trust Keystore Using the Keytool Utility."

     As mentioned in the previous step, this attribute may be optional or required depending on the type of keystore.
8. Click **Save**.
9. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.
10. Click **Lock & Edit**.
11. Select **Configuration**, then **SSL**.
12. 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 Creating an Identity Keystore Using the utils.ImportPrivateKey Utility
13. Click **Save**.
14. Click **Activate Changes** in the Administration Console's Change Center to make the changes take effect.
15. Restart the Administration Server.
16. Restart the Managed Servers where the keystore has been updated.

---

**Note:**

The fact that servers can be restarted using the Administration Console/Node Manager is a good verification that the communication between Node Manager, Administration Server, and the managed servers is correct.

---

## 17.3 Configuring Roles for Administration of an Enterprise Deployment

This section provides a summary of products with specific administration roles and provides instructions to add a product-specific administration role to the Enterprise Deployment Administration group.

Each enterprise deployment consists of multiple products. Some of the products have specific administration users, roles, or groups that are used to control administration access to each product.

However, for an enterprise deployment, which consists of multiple products, you can use a single LDAP-based authorization provider and a single administration user and group to control access to all aspects of the deployment. For more information about creating the authorization provider and provisioning the enterprise deployment administration user and group, see Creating a New LDAP Authenticator and Provisioning a New Enterprise Deployment Administrator User and Group.

To be sure that you can manage each product effectively within the single enterprise deployment domain, you must understand which products require specific administration roles or groups, you must know how to add any specific product administration roles to the single, common enterprise deployment administration group, and if necessary, you must know how to add the enterprise deployment administration user to any required product-specific administration groups.

For more information, see the following topics.

Summary of Products with Specific Administration Roles

Adding a Product-Specific Administration Role to the Enterprise Deployment Administration Group

### 17.3.1 Summary of Products with Specific Administration Roles

The following table lists the Fusion Middleware products that have specific administration roles, which must be added to the enterprise deployment administration group (`WCPAdministrators`), which you defined in the LDAP Authorization Provider for the enterprise deployment.

Use the information in the following table and the instructions in Adding a Product-Specific Administration Role to the Enterprise Deployment Administration Group to add the required administration roles to the enterprise deployment Administration group.

| Product | Application Stripe | Administration Role to be Assigned |
|---|---|---|
| Oracle Web Services Manager | wsm-pm | policy.updater |
| WebCenter Portal | webcenter | s8bba98ff_4cbb_40b8_beee_296c916a23ed#-#Administrator |
| SOA Infrastructure | soa-infra | SOAAdmin |

### 17.3.2 Adding a Product-Specific Administration Role to the Enterprise Deployment Administration Group

For products that require a product-specific administration role, use the following procedure to add the role to the enterprise deployment administration group:

1. Use the Oracle WebLogic Server Administration Server credentials to log in to Oracle Enterprise Manager Fusion Middleware Control.

   These are the credentials you created when you initially configured the domain and created the Oracle WebLogic Server Administration user name (typically, `weblogic_wcp`) and password.

2. From the **WebLogic Domain** menu, select **Security**, and then **Application Roles**.

3. For each production-specific application role, select the corresponding application stripe from the **Application Stripe** drop-down menu.

4. Click Search Application Roles icon to display all the application roles available in the domain.

5. Select the row for the application role you are adding to the enterprise deployment administration group.

6. Click the Edit icon to edit the role.

7. Click the Add icon on the Edit Application Role page.

8. In the Add Principal dialog box, select **Group** from the **Type** drop-down menu.

9. Search for the enterprise deployment administrators group, by entering the group name (for example, `WCPAdministrators`) in the **Principal Name Starts With** field and clicking the right arrow to start the search.

10. Select the administrator group in the search results and click **OK**.

11. Click **OK** on the Edit Application Role page.

## 17.4 Using JDBC Persistent Stores for TLOGs and JMS in an Enterprise Deployment

The following topics provide guidelines for when to use JDBC persistent stores for transaction logs (TLOGs) and JMS. They also provide the procedures you can use to configure the persistent stores in a supported database.



Oracle Fusion Middleware supports both database-based and file-based persistent stores for Oracle WebLogic Server transaction logs (TLOGs) and JMS. Before deciding on a persistent store strategy for your

environment, consider the advantages and disadvantages of each approach.

Products and Components that use JMS Persistence Stores and TLOGs

Performance Impact of the TLOGs and JMS Persistent Stores
One of the primary considerations when selecting a storage method for Transaction Logs and JMS persistent stores is the potential impact on performance. This topic provides some guidelines and details to help you determine the performance impact of using JDBC persistent stores for TLOGs and JMS.

Roadmap for Configuring a JDBC Persistent Store for TLOGs
The following topics describe how to configure a database-based persistent store for transaction logs.

Roadmap for Configuring a JDBC Persistent Store for JMS
The following topics describe how to configure a database-based persistent store for JMS.

Creating a User and Tablespace for TLOGs
Before you can create a database-based persistent store for transaction logs, you must create a user and tablespace in a supported database.

Creating a User and Tablespace for JMS
Before you can create a database-based persistent store for JMS, you must create a user and tablespace in a supported database.

Creating GridLink Data Sources for TLOGs and JMS Stores
Before you can configure database-based persistent stores for JMS and TLOGs, you must create two data sources: one for the TLOGs persistent store and one for the JMS persistent store.

Assigning the TLOGs JDBC store to the Managed Servers
After you create the tablespace and user in the database, and you have created the datasource, you can then assign the TLOGs persistence store to each of the required Managed Servers.

Creating a JDBC JMS Store
After you create the JMS persistent store user and table space in the database, and after you create the data source for the JMS persistent store, you can then use the Administration Console to create the store.

Assigning the JMS JDBC store to the JMS Servers
After you create the JMS tablespace and user in the database, create the JMS datasource, and create the JDBC store, then you can then assign the JMS persistence store to each of the required JMS Servers.

Creating the Required Tables for the JMS JDBC Store
The final step in using a JDBC persistent store for JMS is to create the required JDBC store tables. Perform this task before restarting the Managed Servers in the domain.

## 17.4.1 About JDBC Persistent Stores for JMS and TLOGs

Oracle Fusion Middleware supports both database-based and file-based persistent stores for Oracle WebLogic Server transaction logs (TLOGs) and JMS. Before deciding on a persistent store strategy for your environment, consider the advantages and disadvantages of each approach.

**Note:**

Regardless of which storage method you choose, Oracle recommends that for transaction integrity and consistency, you use the same type of store for both JMS and TLOGs.

When you store your TLOGs and JMS data in an Oracle database, you can take advantage of the replication and high availability features of the database. For example, you can use OracleData Guard to simplify cross-site synchronization. This is especially important if you are deploying Oracle Fusion Middleware in a disaster recovery configuration.

Storing TLOGs and JMS data in a database also means you don't have to identity a specific shared storage location for this data. Note, however, that shared storage is still required for other aspects of an enterprise deployment. For example, it is necessary for Administration Server configuration (to support Administration Server failover), for deployment plans, and for adapter artifacts, such as the File/FTP Adapter control and processed files.

If you are storing TLOGs and JMS stores on a shared storage device, then you can protect this data by using the appropriate replication and backup strategy to guarantee zero data loss, and you will potentially realize better system performance. However, the file system protection will always be inferior to the protection provided by an Oracle Database.

For more information about the potential performance impact of using a database-based TLOGs and JMS store, see Performance Impact of the TLOGs and JMS Persistent Stores.

## 17.4.2 Products and Components that use JMS Persistence Stores and TLOGs

Determining which installed FMW products and components utilize persistent stores can be done through the WebLogic Server Console in the Domain Structure navigation under ***DomainName*** > **Services** > **Persistent Stores**. The list will indicate the name of the store, the store type (usually **FileStore**), the targeted managed server, and whether the target can be migrated to or not.

The persistent stores with migratable targets are the appropriate candidates for consideration of the use of JDBC Persistent Stores. The stores listed that pertain to MDS are outside the scope of this chapter and should not be considered.

Typically, for an Oracle WebCenter Portal environment which includes Oracle WebCenter Content and Oracle SOA, the **WLS_WCC*n*** and **WLS_SOA*n*** managed servers in their respective clusters will be the targets for the JMS and TLOGS data sources and new JDBC Persistent Stores.

## 17.4.3 Performance Impact of the TLOGs and JMS Persistent Stores

One of the primary considerations when selecting a storage method for Transaction Logs and JMS persistent stores is the potential impact on performance. This topic provides some guidelines and details to help you determine the performance impact of using JDBC persistent stores for TLOGs and JMS.

### Performance Impact of Transaction Logs Versus JMS Stores

For transaction logs, the impact of using a JDBC store is relatively small, because the logs are very transient in nature. Typically, the effect is minimal when compared to other database operations in the system.

On the other hand, JMS database stores can have a higher impact on performance if the application is JMS intensive.

#### Factors that Affect Performance

There are multiple factors that can affect the performance of a system when it is using JMS DB stores for custom destinations. The main ones are:

- Custom destinations involved and their type
- Payloads being persisted
- Concurrency on the SOA system (producers on consumers for the destinations)

Depending on the effect of each one of the above, different settings can be configured in the following areas to improve performance:

- Type of data types used for the JMS table (using raw vs. lobs)
- Segment definition for the JMS table (partitions at index and table level)

#### Impact of JMS Topics

If your system uses Topics intensively, then as concurrency increases, the performance degradation with an Oracle RAC database will increase more than for Queues. In tests conducted by Oracle with JMS, the average performance degradation for different payload sizes and different concurrency was less than 30% for Queues. For topics, the impact was more than 40%. Consider the importance of these destinations from the recovery perspective when deciding whether to use database stores.

#### Impact of Data Type and Payload Size

When choosing to use the RAW or SecureFiles LOB data type for the payloads, consider the size of the payload being persisted. For example, when payload sizes range between 100b and 20k, then the amount of database time required by SecureFiles LOB is slightly higher than for the RAW data type.

More specifically, when the payload size reach around 4k, then SecureFiles tend to require more database time. This is because 4k is where writes move out-of-row. At around 20k payload size, SecureFiles data starts being more efficient. When payload sizes increase to more than 20k, then the database time becomes worse for payloads set to the RAW data type.

One additional advantage for SecureFiles is that the database time incurred stabilizes with payload increases starting at 500k. In other words, at that point it is not relevant (for SecureFiles) whether the data is storing 500k, 1MB or 2MB payloads, because the write is asynchronized, and the contention is the same in all cases.

The effect of concurrency (producers and consumers) on the queue's throughput is similar for both RAW and SecureFiles until the payload sizes reeach 50K. For small payloads, the effect on varying concurrency is practically the same, with slightly better scalability for RAW. Scalability is better for SecureFiles when the payloads are above 50k.

#### Impact of Concurrency, Worker Threads, and Database Partioning

Concurrency and worker threads defined for the persistent store can cause contention in the RAC database at the index and global cache level. Using a reverse index when enabling multiple worker threads in one single server or using multiple Oracle WebLogic Server clusters can improve things. However, if the Oracle Database partitioning option is available, then global hash partition for indexes should be used instead. This reduces the contention on the index and the global cache buffer waits,

which in turn improves the response time of the application. Partitioning works well in all cases, some of which will not see significant improvements with a reverse index.

### 17.4.4 Roadmap for Configuring a JDBC Persistent Store for TLOGs

The following topics describe how to configure a database-based persistent store for transaction logs.

1. Creating a User and Tablespace for TLOGs
2. Creating GridLink Data Sources for TLOGs and JMS Stores
3. Assigning the TLOGs JDBC store to the Managed Servers

### 17.4.5 Roadmap for Configuring a JDBC Persistent Store for JMS

The following topics describe how to configure a database-based persistent store for JMS.

1. Creating a User and Tablespace for JMS
2. Creating GridLink Data Sources for TLOGs and JMS Stores
3. Creating a JDBC JMS Store
4. Assigning the JMS JDBC store to the JMS Servers
5. Creating the Required Tables for the JMS JDBC Store

### 17.4.6 Creating a User and Tablespace for TLOGs

Before you can create a database-based persistent store for transaction logs, you must create a user and tablespace in a supported database.

1. Create a tablespace called `tlogs`.

   For example, log in to SQL*Plus as the `sysdba` user and run the following command:

   ```
   SQL> create tablespace tlogs
          logging datafile 'path-to-data-file-or-+asmvolume'
          size 32m autoextend on next 32m maxsize 2048m extent management local;
   ```

2. Create a user named `TLOGS` and assign to it the `tlogs` tablespace.

   For example:

   ```
   SQL> create user TLOGS identified by password;

   SQL> grant create table to TLOGS;

   SQL> grant create session to TLOGS;

   SQL> alter user TLOGS default tablespace tlogs;

   SQL> alter user TLOGS quota unlimited on tlogs;
   ```

### 17.4.7 Creating a User and Tablespace for JMS

Before you can create a database-based persistent store for JMS, you must create a user and tablespace in a supported database.

1. Create a tablespace called `jms`.

   For example, log in to SQL*Plus as the `sysdba` user and run the following command:

   ```
   SQL> create tablespace jms
           logging datafile 'path-to-data-file-or-+asmvolume'
           size 32m autoextend on next 32m maxsize 2048m extent management local;
   ```

2. Create a user named `JMS` and assign to it the `jms` tablespace.

   For example:

   ```
   SQL> create user JMS identified by password;

   SQL> grant create table to JMS;

   SQL> grant create session to JMS;

   SQL> alter user JMS default tablespace jms;

   SQL> alter user JMS quota unlimited on jms;
   ```

## 17.4.8 Creating GridLink Data Sources for TLOGs and JMS Stores

Before you can configure database-based persistent stores for JMS and TLOGs, you must create two data sources: one for the TLOGs persistent store and one for the JMS persistent store.

For an enterprise deployment, you should use GridLink data sources for your TLOGs and JMS stores. To create a GridLink data source:

1. Log in to the Oracle WebLogic Server Administration Console.

2. If you have not already done so, in the **Change Center**, click **Lock & Edit**.

3. In the **Domain Structure** tree, expand **Services**, then select **Data Sources**.

4. On the Summary of Data Sources page, click **New** and select **GridLink Data Source**, and enter the following:

   - Enter a logical name for the data source in the **Name** field.

     For the TLOGs store, enter TLOG; for the JMS store, enter JMS.

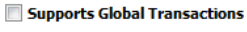
   - Enter a name for **JNDI**.

     For the TLOGs store, enter `jdbc/tlogs`; for the JMS store, enter `jdbc/jms`.

   - For the Database Driver, select **Oracle's Driver (Thin) for GridLink Connections Versions: Any**.

   - Click **Next**.

5. In the Transaction Options page, clear the **Supports Global Transactions** check box, and then click **Next**.



6. In the GridLink Data Source Connection Properties Options screen, select **Enter individual listener information** and click **Next**.

7. Enter the following connection properties:

   - **Service Name**: Enter the service name of the database with lowercase characters. For a GridLink data source, you must enter the Oracle RAC service name. For example:

     `wcpedg.example.com`

   - **Host Name and Port**: Enter the SCAN address and port for the RAC database, separated by a colon. For example:

     `db-scan.example.com:1521`

     Click **Add** to add the host name and port to the list box below the field.


     You can identify the SCAN 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 11*g* Release 1 (11.1), use the virtual IP and port of each database instance listener, for example:

     `dbhost1-vip.mycompany.com (port 1521)`

     and

     `dbhost2-vip.mycompany.com (1521)`

   - **Database User Name**: Enter the following:

     For the TLOGs store, enter `TLOGS`; for the JMS persistent store, enter `JMS`.

   - **Password**: Enter the password you used when you created the user in the database.

   - **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=wcpedg.example.com))) succeeded.
   ```

   Click **Next**.

9. In the ONS Client Configuration page, do the following:

   - Select **FAN Enabled** to subscribe to and process Oracle FAN events.
   - Enter here also the SCAN address: ONS remote port for the RAC database and the ONS remote port as reported by the database (example below) and click **Add**:

     ```
     [orcl@db-scan1 ~]$ srvctl config nodeapps -s

     ONS exists: Local port 6100, remote port 6200, EM port 2016
     ```

   - Click **Next**.

     ---

     **Note:**

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

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

     and

     ```
     custdbhost2.example.com (6200)
     ```

     ---

10. On the Test ONS Client Configuration page, review the connection parameters and click **Test All ONS Nodes**.

    Here is an example of a successful connection notification:

    ```
    Connection test for db-scan.example.com:6200 succeeded.
    ```

    Click **Next**.

11. In the Select Targets page, select the cluster that will be using the persistent store, and then select **All Servers in the cluster**.

12. Click **Finish**.

13. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

14. Repeat step 4 through step 13 to create the GridLink Data Source for JMS File Stores.

### 17.4.9 Assigning the TLOGs JDBC store to the Managed Servers

After you create the tablespace and user in the database, and you have created the datasource, you can then assign the TLOGs persistence store to each of the required Managed Servers.

1. Login in to the Oracle WebLogic Server Administration Console.
2. In the **Change Center**, click **Lock and Edit**.
3. In the Domain Structure tree, expand **Environment**, then **Servers**.
4. Click the name of the Managed Server you want to use the TLOGs store.
5. Select the **Configuration > Services** tab.
6. Under **Transaction Log Store**, select **JDBC** from the **Type** menu.
7. From the **Data Source** menu, select the data source you created for the TLOGs persistence store.
8. In the **Prefix Name** field, specify a prefix name to form a unique JDBC TLOG store name for each configured JDBC TLOG store
9. Click **Save**.
10. Repeat steps 3 to 7 for each of the additional Managed Servers in the cluster.
11. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

### 17.4.10 Creating a JDBC JMS Store

After you create the JMS persistent store user and table space in the database, and after you create the data source for the JMS persistent store, you can then use the Administration Console to create the store.

1. Log in to the Oracle WebLogic Server Administration Console.
2. If you have not already done so, in the **Change Center**, click **Lock & Edit**.
3. In the **Domain Structure** tree, expand **Services**, then select **Persistent Store**.
4. Click **New**, and then click **Create JDBCStore**.
5. Enter a persistent store name that easily relates it to the pertaining JMS servers that will be using it.
6. Specify a unique prefix qualifying the installation and cluster and associate it with the data source you created for the JMS persistent store.

   There is a 30 character limit of the table field value, this includes the prefix and the value of `WLSTORE`, which WebLogic adds. Therefore, the limit for the prefix should be 23 characters.
7. Target the store to the entity that will host the JTA services.

In the case of a server using service migration, this will be the migratable target to which the JMS server belongs.

There must be an individual JMS Store created for each existing file-based store, which needs to be configured for JDBC.

8. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

## 17.4.11 Assigning the JMS JDBC store to the JMS Servers

After you create the JMS tablespace and user in the database, create the JMS datasource, and create the JDBC store, then you can then assign the JMS persistence store to each of the required JMS Servers.

1. Login in to the Oracle WebLogic Server Administration Console.
2. In the **Change Center**, click **Lock and Edit**.
3. In the Domain Structure tree, expand **Services**, then **Messaging**, then **JMS Servers**.
4. Click the name of the JMS Server that you want to use the persistent store.
5. From the **Persistent Store** menu, select the JMS persistent store you created earlier.
6. Click **Save**.
7. Repeat steps 3 to 6 for each of the additional JMS Servers in the cluster.
8. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

## 17.4.12 Creating the Required Tables for the JMS JDBC Store

The final step in using a JDBC persistent store for JMS is to create the required JDBC store tables. Perform this task before restarting the Managed Servers in the domain.

1. Use the find command to locate the WLS core jdbc store library and extract the DDL files to a temporary directory using the jar utility supplied with the JDK.

```
mkdir /tmp/edgddl
cd /tmp/edgddl
JAVA_HOME/bin/jar xvf WL_HOME/modules/com.bea.core.store.jdbc.jar weblogic/
store/io/jdbc/ddl/
```

---

**Note:** This will extract several ddl files for the various supported database platforms and several for Oracle DB to choose from based on features desired.

---

---

**Note:**

If you omit the `weblogic/store/io/jdbc/ddl` parameter, then the entire jar file is extracted.

---

2. Review the information in Performance Impact of the TLOGs and JMS Persistent Stores, and decide which table features are appropriate for your environment..

   There are three oracle DB schema definitions provided in this release and were extracted for review in the previous step. The basic definition includes the RAW

data type without any partition for indexes. The second uses the blob data type, and the third uses the blob data type and secure files.

3. Create a domain-specific well-named folder structure for the custom DDL file on shared storage. The ORACLE_RUNTIME shared volume is recommended so it is available to all servers.

   Example:

   ```
   mkdir -p ORACLE_RUNTIME/domain_name/ddl
   ```

4. Create a `jms_custom.ddl` file in new shared ddl folder based on your requirements analysis.

   For example, to implement an optimized schema definition that uses both secure files and hash partitioning, create the jms_custom.ddl file with the following content:

   ```
   CREATE TABLE $TABLE (
     id     int  not null,
     type   int  not null,
     handle int  not null,
     record blob not null,
   PRIMARY KEY (ID) USING INDEX GLOBAL PARTITION BY HASH (ID) PARTITIONS 8)
   LOB (RECORD) STORE AS SECUREFILE (ENABLE STORAGE IN ROW);
   ```

   This example can be compared to the default schema definition for JMS stores, where the RAW data type is used without any partitions for indexes.

   Note that the number of partitions should be a power of two. This will ensure that each partition will be a similar size. The recommended number of partitions will vary depending on the expected table or index growth. You should have your database administrator (DBA) analyze the growth of the tables over time and adjust the tables accordingly. For more information, see the Oracle Database VLDB and Partitioning Guide.

5. Clean up the custom directory and files extracted to the **tmp** directory in step 1 earlier.

6. Use the Administration Console to edit the existing JDBC Store you created earlier; create the table that will be used for the JMS data:

   a. Login in to the Oracle WebLogic Server Administration Console.

   b. In the **Change Center**, click **Lock and Edit**.

   c. In the Domain Structure tree, expand **Services**, then **Persistent Stores**.

   d. Click the persistent store you created earlier.

   e. Under the **Advanced** options, enter *`ORACLE_RUNTIME/domain_name/`*`ddl/jms_custom.ddl` in the **Create Table from DDL File** field.

   f. Click **Save**.

   g. To activate these changes, in the Change Center of the Administration Console, click **Activate Changes**.

7. Restart the Managed Servers.

## 17.5 Performing Backups and Recoveries for an Enterprise Deployment

This section provides guidelines for making sure you back up the necessary directories and configuration data for an Oracle WebCenter Portal enterprise deployment.

---

**Note:**

Some of the static and run-time artifacts listed in this section are hosted from Network Attached Storage (NAS). If possible, backup and recover these volumes from the NAS filer directly rather than from the application servers.

---

For general information about backing up and recovering Oracle Fusion Middleware products, see the following sections in *Administering Oracle Fusion Middleware*:

- "Backing Up Your Environment"
- "Recovering Your Environment"

Table 17-1 lists the static artifacts to back up in a typical Oracle WebCenter Portal enterprise deployment.

***Table 17-1 Static Artifacts to Back Up in the Oracle WebCenter Portal Enterprise Deployment***

| Type | Host | Tier |
|---|---|---|
| Database Oracle home | DBHOST1 and DBHOST2 | Data Tier |
| Oracle Fusion Middleware Oracle home | WEBHOST1 and WEBHOST2 | Web Tier |
| Oracle Fusion Middleware Oracle home | WCPHOST1 and WCPHOST2 | Application Tier |
| Installation-related files | WEBHOST1, WEHOST2, and shared storage | N/A |

Table 17-2 lists the runtime artifacts to back up in a typical Oracle WebCenter Portal enterprise deployment.

***Table 17-2 Run-Time Artifacts to Back Up in the Oracle WebCenter Portal Enterprise Deployment***

| Type | Host | Tier |
|---|---|---|
| Administration Server domain home (ASERVER_HOME) | WCPHOST1 and WCPHOST2 | Application Tier |
| Application home (APPLICATION_HOME) | WCPHOST1 and WCPHOST2 | Application Tier |
| Oracle RAC databases | DBHOST1 and DBHOST2 | Data Tier |
| Scripts and Customizations | WCPHOST1 and WCPHOST2 | Application Tier |
| Deployment Plan home (DEPLOY_PLAN_HOME) | WCPHOST1 and WCPHOST2 | Application Tier |

***Table 17-2 (Cont.) Run-Time Artifacts to Back Up in the Oracle WebCenter Portal Enterprise Deployment***

| Type | Host | Tier |
|---|---|---|
| OHS Configuration directory | WEBHOST1 and WEBHOST2 | Web Tier |

# 18

# Using Whole Server Migration and Service Migration in an Enterprise Deployment

The following topics describe Oracle WebLogic Server Whole Server migration and Oracle WebLogic Server Automatic Service Migration. The also explain how these features can be used in an Oracle Fusion Middleware enterprise topology.

About Whole Server Migration and Automatic Service Migration in an Enterprise Deployment
: Oracle WebLogic Server provides a migration framework that is integral part of any highly available environment. The following sections provide more information about how this framework can be used effectively in an enterprise deployment.

Creating a GridLink Data Source for Leasing
: Both Whole Server Migration and Automatic Service Migration require a data source for the leasing table, which is a tablespace created automatically as part of the Oracle WebLogic Server schemas by the Repository Creation Utility (RCU).

Configuring Whole Server Migration for an Enterprise Deployment
: After you have prepared your domain for whole server migration or automatic service migration, you can then configure Whole Server Migration for specific Managed Servers within a cluster. See the following topics for more information.

Configuring Automatic Service Migration in an Enterprise Deployment
: To configure automatic service migration for specific services in an enterprise deployment, refer to the topics in this section.

## 18.1 About Whole Server Migration and Automatic Service Migration in an Enterprise Deployment

Oracle WebLogic Server provides a migration framework that is integral part of any highly available environment. The following sections provide more information about how this framework can be used effectively in an enterprise deployment.

Understanding the Difference Between Whole Server and Service Migration

Implications of Using Whole Server Migration or Service Migration in an Enterprise Deployment

Understanding Which Products and Components Require Whole Server Migration and Service Migration

### 18.1.1 Understanding the Difference Between Whole Server and Service Migration

The Oracle WebLogic Server migration framework supports two distinct types of automatic migration:

- **Whole Server Migration**, where the Managed Server instance is migrated to a different physical system upon failure.

  Whole server migration provides for the automatic restart of a server instance, with all of its services, on a different physical machine. When a failure occurs in a server that is part of a cluster that is configured with server migration, the server is restarted on any of the other machines that host members of the cluster.

  For this to happen, the servers need to use a a floating IP as listen address and the required resources (transactions logs and JMS persistent stores) must be available on the candidate machines.

  For more information, see "Whole Server Migration" in *Administering Clusters for Oracle WebLogic Server*.

- **Service Migration**, where specific services are moved to a different Managed Server within the cluster.

  To understand service migration, it's important to understand *pinned services*.

  In a WebLogic Server cluster, most subsystem services are hosted homogeneously on all server instances in the cluster, enabling transparent failover from one server to another. In contrast, pinned services, such as JMS-related services, the JTA Transaction Recovery Service, and user-defined singleton services, are hosted on individual server instances within a cluster—for these services, the WebLogic Server migration framework supports failure recovery with service migration, as opposed to failover.

  For more information, see "Understanding the Service Migration Framework" in *Administering Clusters for Oracle WebLogic Server*.

### 18.1.2 Implications of Using Whole Server Migration or Service Migration in an Enterprise Deployment

When a server or service is started in another system, the required resources (such as services data and logs) must be available to both the original system and to the failover system; otherwise, the service cannot resume the same operations successfully on the failover system.

For this reason, both whole server and service migration require that all members of the cluster have access to the same transaction and JMS persistent stores (whether the persistent store is file-based or database-based).

This is another reason why shared storage is important in an enterprise deployment. When you properly configure shared storage, you ensure that in the event of a manual failover (Administration Server failover) or an automatic failover (whole server migration or service migration), both the original machine and the failover machine can access the same file store with no change in service.

In the case of an automatic service migration, when a pinned service needs to be resumed, the JMS and JTA logs that it was using before failover need to be accessible.

In addition to shared storage, Whole Server Migration requires the procurement and assignment of a virtual IP address (VIP). When a Managed Server fails over to another machine, the VIP is automatically reassigned to the new machine.

Note that service migration does not require a VIP.

### 18.1.3 Understanding Which Products and Components Require Whole Server Migration and Service Migration

The following table summarizes the list of FMW products and components that benefit from use of a migration capability and indicates the best-practice recommendation for this release. Components listed as migratable can use either Whole Server or Automatic Service Migration.

Note that the table lists the recommended best practice. It does not preclude you from using Whole Server or Automatic Server Migration for those components that support it.

| Component | Whole Server Migration (WSM) | Automatic Service Migration (ASM) |
|---|---|---|
| Oracle Web Services Manager (OWSM) | NO | NO |
| Oracle WebCenter Portal | NO | NO |
| Oracle WebCenter Portal Portlets and Pagelet Producers | NO | NO |
| Oracle WebCenter Content | YES | YES (Recommended) |
| Oracle WebCenter Inbound Refinery | NO | NO |
| Oracle SOA Suite | YES | YES (Recommended) |
| Oracle Enterprise Scheduler | NO | NO |

## 18.2 Creating a GridLink Data Source for Leasing

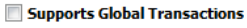
Both Whole Server Migration and Automatic Service Migration require a data source for the leasing table, which is a tablespace created automatically as part of the Oracle WebLogic Server schemas by the Repository Creation Utility (RCU).

For an enterprise deployment, you should use create a GridLink data source:

1. Log in to the Oracle WebLogic Server Administration Console.
2. If you have not already done so, in the **Change Center**, click **Lock & Edit**.
3. In the **Domain Structure** tree, expand **Services**, then select **Data Sources**.
4. On the Summary of Data Sources page, click **New** and select **GridLink Data Source**, and enter the following:
   - 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: Any**.
- Click **Next**.

5. In the Transaction Options page, clear the **Supports Global Transactions** check box, and then click **Next**.




6. In the GridLink Data Source Connection Properties Options screen, select **Enter individual listener information** and click **Next**.

7. Enter the following connection properties:

   - **Service Name**: Enter the service name of the database with lowercase characters. For a GridLink data source, you must enter the Oracle RAC service name. For example:

     ```
     wcpedg.example.com
     ```

   - **Host Name and Port**: Enter the SCAN address and port for the RAC database, separated by a colon. For example:

     ```
     db-scan.example.com:1521
     ```

     Click **Add** to add the host name and port to the list box below the field.


     You can identify the SCAN 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 11*g* Release 1 (11.1), use the virtual IP and port of each database instance listener, for example:

```
dbhost1-vip.mycompany.com (port 1521)
```

and

```
dbhost2-vip.mycompany.com (1521)
```

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

- **Database User Name**: Enter the following:

  ```
  FMW1221_WLS_RUNTIME
  ```

  In this example, FMW1221 is the prefix you used when you created the schemas as you prepared to configure the initial enterprise manager domain.

  Note that in previous versions of Oracle Fusion Middleware, you had to manually create a user and tablespace for the migration leasing table. In Fusion Middleware 12*c* (12.2.1), the leasing table is created automatically when you create the WLS schemas with the Repository Creation Utility (RCU).

- **Password**: Enter the password you used when you created the WLS schema in RCU.

- **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=wcpedg.example.com))) succeeded.
   ```

   Click **Next**.

9. In the ONS Client Configuration page, do the following:

   - Select **FAN Enabled** to subscribe to and process Oracle FAN events.

   - Enter the SCAN address in the **ONS Host and Port** field, and then click **Add** and click **Add**:

     This value should be the ONS host and ONS remote port for the RAC database. To find the ONS remote port for the database, you can use the following command on the database host:

     ```
     [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* Release 1 (11.1), use the hostname and port of each database's ONS service, for example:

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

and

```
custdbhost2.example.com (6200)
```

10. On the Test ONS Client Configuration page, review the connection parameters and click **Test All ONS Nodes**.

    Here is an example of a successful connection notification:

    ```
    Connection test for db-scan.example.com:6200 succeeded.
    ```

    Click **Next**.

11. In the Select Targets page, select the cluster that you are configuring for Whole Server Migration or Automatic Service Migration, and then select **All Servers in the cluster**.

12. Click **Finish**.

13. Click **Activate Changes**.

## 18.3 Configuring Whole Server Migration for an Enterprise Deployment

After you have prepared your domain for whole server migration or automatic service migration, you can then configure Whole Server Migration for specific Managed Servers within a cluster. See the following topics for more information.

Editing the Node Manager's Properties File to Enable Whole Server Migration

Setting Environment and Superuser Privileges for the wlsifconfig.sh Script

Configuring Server Migration Targets

Testing Whole Server Migration

### 18.3.1 Editing the Node Manager's Properties File to Enable Whole Server Migration

Use the section to edit the Node Manager properties file on the two nodes where the servers are running.

1. Locate and open the following file with a text editor:

   *MSERVER_HOME*`/nodemanager/nodmeanager.properties`

2. If not done already, set the `StartScriptEnabled` property in the `nodemanager.properties` file to true.

   This is required to enable Node Manager to start the managed servers.

3. Add the following properties to the `nodemanager.properties` file to enable server migration to work properly:

- `Interface`

  ```
  Interface=eth0
  ```

  This property specifies the interface name for the floating IP (`eth0`, for example).

  **Note:**

  Do not specify the sub interface, such as `eth0:1` or `eth0:2`. This interface is to be used without the `:0`, or `:1`.

  The Node Manager's scripts traverse the different `:X` enabled IPs to determine which to add or remove. For example, the valid values in Linux environments are `eth0`, `eth1`, or, `eth2`, `eth3`, `eth`*n*, depending on the number of interfaces configured.

- `NetMask`

  ```
  NetMask=255.255.255.0
  ```

  This property specifies the net mask for the interface for the floating IP.

- `UseMACBroadcast`

  ```
  UseMACBroadcast=true
  ```

  This property specifies whether or not to use a node's MAC address when sending ARP packets, that is, whether or not to use the `-b` flag in the arping command.

4. Restart the Node Manager.

5. Verify in the output of Node Manager (the shell where the Node Manager is started) that these properties are in use. Otherwise, problems may occur during migration. The output should be similar to the following:

   ```
   ...
   SecureListener=true
   LogCount=1
   eth0=*,NetMask=255.255.255.0
   ...
   ```

## 18.3.2 Setting Environment and Superuser Privileges for the wlsifconfig.sh Script

Use this section to set the environment and superuser privileges for the `wlsifconfig.sh` script, which is used to transfer IP addresses from one machine to another during migration. It must be able to run `ifconfig`, which is generally only available to superusers.

For more information about the `wlsifconfig.sh` script, see "Configuring Automatic Whole Server Migration" in *Administering Clusters for Oracle WebLogic Server*.

Refer to the following sections for instructions on preparing your system to run the `wlsifconfig.sh` script.

Setting the PATH Environment Variable for the wlsifconfig.sh Script

Granting Privileges to the wlsifconfig.sh Script

#### 18.3.2.1 Setting the PATH Environment Variable for the wlsifconfig.sh Script

Ensure that the commands listed in the following table are included in the PATH environment variable for each host computers.

| File | Directory Location |
|---|---|
| `wlsifconfig.sh` | *MSERVER_HOME*`/bin/server_migration` |
| `wlscontrol.sh` | *WL_HOME*`/common/bin` |
| `nodemanager.domains` | *MSERVER_HOME*`/nodemanager` |

#### 18.3.2.2 Granting Privileges to the wlsifconfig.sh Script

Grant sudo privilege to the operating system user (for example, `oracle`) with no password restriction, and grant execute privilege on the `/sbin/ifconfig` and `/sbin/arping` binaries.

**Note:**

For security reasons, `sudo` should be restricted to the subset of commands required to run the `wlsifconfig.sh` script.

Ask the system administrator for the sudo and system rights as appropriate to perform this required configuration task.

The following is an example of an entry inside */etc/sudoers* granting sudo execution privilege for `oracle` to run `ifconfig` and `arping`:

```
Defaults:oracle !requiretty
oracle ALL=NOPASSWD: /sbin/ifconfig,/sbin/arping
```

### 18.3.3 Configuring Server Migration Targets

To configure migration in a cluster:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand **Environment** and select **Clusters**. The Summary of Clusters page appears.
3. Click the cluster for which you want to configure migration in the Name column of the table.
4. Click the **Migration** tab.
5. Click **Lock & Edit**.
6. Select **Database** as Migration Basis. From the drop-down list, select **Leasing** as Data Source For Automatic Migration.

7. Under **Candidate Machines For Migratable Server**, in the Available filed, select the Managed Servers in the cluster and click the right arrow to move them to **Chosen**.
8. Select the Leasing data source that you created in Creating a GridLink Data Source for Leasing.
9. Click **Save**.
10. Set the Candidate Machines for Server Migration. You must perform this task for all of the managed servers as follows:
    a. In Domain Structure window of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Servers**.
    b. Select the server for which you want to configure migration.
    c. Click the **Migration** tab.
    d. Select **Automatic Server Migration Enabled** and click **Save**.

       This enables the Node Manager to start a failed server on the target node automatically.

       For information on targeting applications and resources, see Using Multi Data Sources with Oracle RAC.
    e. In the **Available** field, located in the Migration Configuration section, select the machines to which to allow migration and click the right arrow.

       In this step, you are identifying host to which the Managed Server should failover if the current host is unavailable. For example, for the Managed Server on the HOST1, select HOST2; for the Managed Server on HOST2, select HOST1.

       **Tip:**

       Click **Customize this table** in the Summary of Servers page, move Current Machine from the Available Window to the Chosen window to view the machine on which the server is running. This is different from the configuration if the server is migrated automatically.
11. Click **Activate Changes**.
12. Restart the Administration Server and the servers for which server migration has been configured.

## 18.3.4 Testing Whole Server Migration

Perform the steps in this section to verify that automatic whole server migration is working properly.

**To test from Node 1:**

1. Stop the managed server process.

   ```
   kill -9 pid
   ```

   *pid* specifies the process ID of the managed server. You can identify the pid in the node by running this command:

```
ps -ef | grep WC_Portal1
```

2. Watch the Node Manager console (the terminal window where you performed the kill command): you should see a message indicating that the managed server's floating IP has been disabled.

3. Wait for the Node Manager to try a second restart of the Managed Server. Node Manager waits for a period of 30 seconds before trying this restart.

4. After node manager restarts the server and before it reaches "RUNNING" state, kill the associated process again.

   Node Manager should log a message indicating that the server will not be restarted again locally.

---

**Note:**

The number of restarts required is determined by the `RestartMax` parameter in the following configuration file:

*MSERVER_HOME*`/servers/WC_Portal1/data/nodemanager/startup.properties`

The default value is `RestartMax=2`.

---

**To test from Node 2:**

1. Watch the local Node Manager console. After 30 seconds since the last try to restart the managed server on Node 1, Node Manager on Node 2 should prompt that the floating IP for the managed server is being brought up and that the server is being restarted in this node.

2. Access a product URL using same IP address. If the URL is successful, then the migration was successful.

### Verification From the Administration Console

You can also verify migration using the Oracle WebLogic Server Administration Console:

1. Log in to the Administration Console.

2. Click **Domain** on the left console.

3. Click the **Monitoring** tab and then the **Migration** subtab.

   The Migration Status table provides information on the status of the migration.

---

**Note:**

After a server is migrated, to fail it back to its original machine, stop the managed server from the Oracle WebLogic Administration Console and then start it again. The appropriate Node Manager starts the managed server on the machine to which it was originally assigned.

---

# 18.4 Configuring Automatic Service Migration in an Enterprise Deployment

To configure automatic service migration for specific services in an enterprise deployment, refer to the topics in this section.



## 18.4.1 Setting the Leasing Mechanism and Data Source for an Enterprise Deployment Cluster

Before you can configure automatic service migration, you must verify the leasing mechanism and data source that will be used by the automatic service migration feature:

---

**Note:**

The following procedure assumes you have already created the Leasing data source, as described in Creating a GridLink Data Source for Leasing.

---

1. Log in to the Oracle WebLogic Server Administration Console.
2. Click **Lock & Edit**.
3. In the Domain Structure window, expand **Environment** and select **Clusters**.

   The Summary of Clusters page appears.
4. In the **Name** column of the table, click the cluster for which you want to configure migration.
5. Click the **Migration** tab.
6. Verify that **Database** is selected in the **Migration Basis** drop-down menu.
7. From the **Data Source for Automatic Migration** drop-down menu, select the Leasing data source that you created in Creating a GridLink Data Source for Leasing.
8. Click **Save**.
9. Activate changes.
10. Restart the Managed Servers.

## 18.4.2 Changing the Migration Settings for the Managed Servers in the Cluster

After you set the leasing mechanism and data source for the cluster, you can then enable automatic JTA migration for the Managed Servers that you want to configure for service migration. Note that this topic applies only if you are deploying JTA services as part of your enterprise deployment.

To change the migration settings for the Managed Servers in each cluster:

1. If you haven't already, log in to the Administration Console, and click **Lock & Edit**.
2. In the Domain Structure pane, expand the **Environment** node and then click **Servers**.

   The Summary of Servers page appears.
3. Click the name of the server you want to modify in **Name** column of the table.

   The settings page for the selected server appears and defaults to the Configuration tab.
4. Click the **Migration** tab.
5. From the **JTA Migration Policy** drop-down menu, select **Failure Recovery**.
6. In the **JTA Candidate Servers** section of the page, select the Managed Servers in the **Available** list box, and then click the move button to move them into the **Chosen** list box.
7. In the **JMS Service Candidate Servers** section of the page, select the Managed Servers in the **Available** list box, and then click the move button to move them into the **Chosen** list box.
8. Click **Save**.
9. Restart all the Managed Servers and the Administration Server.

## 18.4.3 About Selecting a Service Migration Policy

When you configure Automatic Service Migration, you select a Service Migration Policy for each cluster. This topic provides guidelines and considerations when selecting the Service Migration Policy.

For example, products or components running singletons or using Path services can benefit from the **Auto-Migrate Exactly-Once** policy. With this policy, if at least one Managed Server in the candidate server list is running, the services hosted by this migratable target will be active somewhere in the cluster if servers fail or are administratively shut down (either gracefully or forcibly). This can cause multiple homogenous services to end up in one server on startup.

When you are using this policy, you should monitor the cluster startup to identify what servers are running on each server. You can then perform a manual failback, if necessary, to place the system in a balanced configuration.

Other Fusion Middleware components are better suited for the **Auto-Migrate Failure-Recovery Services** policy.

Based on these guidelines, you should use **Auto-Migration Failure-Recovery Services** for the clusters in an Oracle WebCenter Content enterprise deployment.

For more information, see Policies for Manual and Automatic Service Migration in *Administering Clusters for Oracle WebLogic Server*.

### 18.4.4 Setting the Service Migration Policy for Each Managed Server in the Cluster

After you modify the migration settings for each server in the cluster, you can then identify the services and set the migration policy for each Managed Server in the cluster, using the WebLogic Administration Console:

1. If you haven't already, log in to the Administration Console, and click **Lock & Edit**.
2. In the Domain Structure pane, expand **Environment**, then expand **Clusters**, then select **Migratable Targets**.
3. Click the name of the first Managed Server in the cluster.
4. Click the **Migration** tab.
5. From the **Service Migration Policy** drop-down menu, select the appropriate policy for the cluster.

   For more information, see About Selecting a Service Migration Policy.
6. Click **Save**.
7. Repeat steps 2 through 6 for each of the additional Managed Servers in the cluster.
8. Activate the changes.
9. Restart the Managed Servers in the cluster.

### 18.4.5 Restarting the Managed Servers and Validating Automatic Service Migration

After you configure automatic service migration for your cluster and Managed Servers, validate the configuration, as follows:

1. If you haven't already, log in to the Administration Console.
2. In the Domain Structure pane, select **Environment**, then **Clusters**, and restart the cluster you just configured for automatic service migration.
3. In the Domain Structure pane, expand **Environment**, and then expand **Clusters**.
4. Click **Migratable Targets**.
5. Click the **Control** tab.

   The console displays a list of migratable targets and their current hosting server.
6. In the Migratable Targets table, select a row for the one of the migratable targets.
7. Note the value in the **Current Hosting Server** column.
8. Use the operating system command line to stop the first Managed Server.

   Use the following command to kill the Managed Server Process and simulate a crash scenario:

   ```
   kill -9 pid
   ```

In this example, replace *pid* with the process ID (PID) of the Managed Server. You can identify the PID by running the following UNIX command:

```
ps -ef | grep managed_server_name
```

Note that after you kill the process, the Managed Server might be configured to start automatically after you initially kill the process. In this case, you must kill the second process using the `kill -9` command again.

9. Watch the terminal window (or console) where the Node Manager is running.

   You should see a message indicating that the selected Managed Server has failed. The message will be similar to the following:

```
<INFO> <domain_name> <server_name>
<The server 'server_name' with process id 4668 is no longer alive; waiting for
the process to die.>
<INFO> <domain_name> <server_name>
<Server failed so attempting to restart (restart count = 1)>.
```

10. Return to the Oracle WebLogic Server Administration Console and refresh the table of migratable targets; verify that the migratable targets are transferred to the remaining, running Managed Server in the cluster:

    - Verify that the Current Hosting Server for the process you killed is now updated to show that it has been migrated to a different host.
    - Verify that the value in the **Status of Last Migration** column for the process is "Succeeded".

11. Open and review the log files for the Managed Servers that are now hosting the services; look for any JTA or JMS errors.

---

**Note:**

For JMS tests, it is a good practice to get message counts from destinations and make sure that there are no stuck messages in any of the migratable targets:

For example, for uniform distributed destinations (UDDs):

**a.** Access the JMS Subdeployment module in the Administration Console:

In the Domain Structure pane, select **Services**, then **Messaging**, and then **JMS Modules**.

**b.** Click the JMS Module.

**c.** Click the destination in the **Summary of Resources** table. destination->Select monitoring and get the Messages Total and Messages Pending Counts

**d.** Select the Monitoring tab, and review the **Messages Total** and **Messages Pending** values in the **Destinations** table.

---

## 18.4.6 Failing Back Services After Automatic Service Migration

When Automatic Service Migration occurs, Oracle WebLogic Server does not support failing back services to their original server when a server is back online and rejoins the cluster.

As a result, after the Automatic Service Migration migrates specific JMS services to a backup server during a fail-over, it does not migrate the services back to the original server after the original server is back online. Instead, you must migrate the services back to the original server manually.

To fail back a service to its original server, follow these steps:

1. If you have not already done so, in the Change Center of the Administration Console, click **Lock & Edit.**
2. In the Domain Structure tree, expand **Environment**, expand **Clusters**, and then select **Migratable Targets**.
3. To migrate one or more migratable targets at once, on the Summary of Migratable Targets page:
   a. Click the **Control** tab.
   b. Use the check boxes to select one or more migratable targets to migrate.
   c. Click **Migrate**.
   d. Use the **New hosting server** drop-down to select the original Managed Server.
   e. Click **OK**.

      A request is submitted to migrate the JMS-related service and the configuration edit lock is released. In the Migratable Targets table, the Status of Last Migration column indicates whether the requested migration has succeeded or failed.
4. To migrate a specific migratable target, on the Summary of Migratable Targets page:
   a. Select the migratable target to migrate.
   b. Click the **Control** tab.
   c. Reselect the migratable target to migrate.
   d. Click **Migrate**.
   e. Use the New hosting server drop-down to select a new server for the migratable target.
   f. Click **OK**.

# 19

# Configuring Single Sign-On for an Enterprise Deployment

This chapter describes how to configure the Oracle HTTP Server WebGate to enable single sign-on with Oracle Access Manager.

## 19.1 About Oracle HTTP Server Webgate

Oracle HTTP Server WebGate is a Web server plug-in that intercepts HTTP requests and forwards them to an existing Oracle Access Manager instance for authentication and authorization.

For Oracle Fusion Middleware 12*c*, the WebGate software is installed as part of the Oracle HTTP Server 12*c* software installation.

For more extensive information about WebGate, see Registering and Managing OAM 11g Agents in *Adminstrator's Guide for Oracle Access Management*.

## 19.2 General Prerequisites for Configuring Oracle HTTP Server Webgate

Before you can configure Oracle HTTP Server WebGate, you must have installed and configured a certified version of Oracle Access Manager.

At the time this document was published, the supported versions of Oracle Access Manager were 11*g* Release 2 (11.1.2.2) and 11*g* Release 2 (11.1.2.3). For the most up-to-date information, see the certification document for your release on the *Oracle Fusion Middleware Supported System Configurations* page.

---

**Note:**

For production environments, it is highly recommended that you install Oracle Access Manager in its own environment and not on the machines that are hosting the enterprise deployment.

---

For more information about Oracle Access Manager, see the latest Oracle Identity and Access Management documentation, which you can find in the **Middleware** documentation on the Oracle Help Center.

## 19.3 Enterprise Deployment Prerequisites for Configuring OHS 12*c* Webgate

When you are configuring Oracle HTTP Server Webgate to enable Single Sign-On for an enterprise deployment, consider the prerequisites mentioned in this section.

- Oracle recommends that you deploy Oracle Access Manager as part of a highly available, secure, production environment. For more information about deploying Oracle Access Manager in an enterprise environment, see the Enterprise Deployment Guide for your version of Oracle Identity and Access Mangement.
- To enable single sign-on for the WebLogic Server Administration Console and the Oracle Enterprise Manager Fusion Middleware Control, you must add a central LDAP-provisioned administration user to the directory service that Oracle Access Manager is using (for example, Oracle Internet Directory or Oracle Unified Directory). For more information about the required user and groups to add to the LDAP directory, follow the instructions in Creating a New LDAP Authenticator and Provisioning Enterprise Deployment Users and Group.

## 19.4 Configuring Oracle HTTP Server 12*c* WebGate for an Enterprise Deployment

Perform the following steps to configure Oracle HTTP Server 12*c* WebGate for Oracle Access Manager on both WEBHOST1 and WEBHOST2.

In the following procedure, replace the directory variables, such as *OHS_ORACLE_HOME* and *OHS_CONFIG_DIR*, with the values, as defined in File System and Directory Variables Used in This Guide.

1. Perform a complete backup of the Web Tier domain.
2. Change directory to the following location in the Oracle HTTP Server Oracle home:

   ```
   cd OHS_ORACLE_HOME/webgate/ohs/tools/deployWebGate/
   ```

3. Run the following command to create the WebGate Instance directory and enable WebGate logging on OHS Instance:

   ```
   ./deployWebGateInstance.sh -w OHS_CONFIG_DIR -oh OHS_ORACLE_HOME
   ```

4. Verify that a `webgate` directory and subdirectories was created by the `deployWebGateInstance` command:

   ```
   ls -lart OHS_CONFIG_DIR/webgate/
   total 16
   drwxr-x---+ 8 orcl oinstall 20 Oct  2 07:14 ..
   drwxr-xr-x+ 4 orcl oinstall  4 Oct  2 07:14 .
   drwxr-xr-x+ 3 orcl oinstall  3 Oct  2 07:14 tools
   drwxr-xr-x+ 3 orcl oinstall  4 Oct  2 07:14 config
   ```

5. Run the following command to ensure that the `LD_LIBRARY_PATH` environment variable contains *`OHS_ORACLE_HOME`*`/lib` directory path:

   ```
   export LD_LIBRARY_PATH=OHS_ORACLE_HOME/lib
   ```

   If `LD_LIBRARY_PATH` is already set, run the following command:

   ```
   export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:OHS_ORACLE_HOME/lib
   ```

6. Change directory to the following directory

   *`OHS_ORACLE_HOME`*`/webgate/ohs/tools/setup/InstallTools`

7. Run the following command from the `InstallTools` directory.

   ```
   ./EditHttpConf -w OHS_CONFIG_DIR -oh OHS_ORACLE_HOME -o
   output_file_name
   ```

   **Note:**

   The `-oh` *`OHS_ORACLE_HOME`* and `-o` *`output_file_name`* parameters are optional.

   This command:

- Copies the `apache_webgate.template` file from the Oracle HTTP Server Oracle home to a new `webgate.conf` file in the Oracle HTTP Server configuration directory.
- Updates the `httpd.conf` file to add one line, so it includes the `webgate.conf`.
- Generates a WebGate configuration file. The default name of the file is `webgate.conf`, but you can use a custom name by using the *`output_file`* argument to the command.

## 19.5 Registering the Oracle HTTP Server WebGate with Oracle Access Manager

You can register the WebGate agent with Oracle Access Manager using the Oracle Access Manager Administration console.

For more information, see Registering an OAM Agent Using the Console in *Administrator's Guide for Oracle Access Management*.



### 19.5.1 About RREG In-Band and Out-of-Band Mode

You can run the RREG Tool in one of two modes: in-band and out-of-band.

Use **in-band** mode when you have the privileges to access the Oracle Access Manager server and run the RREG tool yourself from the Oracle Access Manager Oracle home. You can then copy the generated artifacts and files to the Web server configuration directory after you run the RREG Tool.

Use **out-of-band** mode if you do *not* have privileges or access to the Oracle Access Manager server. For example, in some organizations, only the Oracle Access Manager server administrators have privileges access the server directories and perform administration tasks on the server. In out-of-band mode, the process can work as follows:

1. The Oracle Access Manager server administrator provides you with a copy of the RREG archive file (RREG.tar.gz).
2. Untar the `RREG.tar.gz` file that was provided to you by the server administrator.

   For example:

   ```
   gunzip RREG.tar.gz
   ```

```
tar -xvf RREG.tar
```

After you unpack the RREG archive, you can find the tool for registering the agent in the following location:

*RREG_HOME*/bin/oamreg.sh

In this example, *RREG_Home* is the directory in which you extracted the contents of RREG archive.

3. Use the instructions in Updating the Standard Properties in the OAM11gRequest.xml File to update the `OAM11GRequest.xml` file, and send the completed `OAM11GRequest.xml` file to the Oracle Access Manager server administrator.

4. The Oracle Access Manager server administrator then uses the instructions in Running the RREG Tool in Out-Of-Band Mode to run the RREG Tool and generate the *AgentID*`_response.xml` file.

5. The Oracle Access Manager server administrator sends the *AgentID*`_response.xml` file to you.

6. Use the instructions in Running the RREG Tool in Out-Of-Band Mode to run the RREG Tool with the *AgentID*`_response.xml` file and generate the required artifacts and files on the client system.

## 19.5.2 Updating the Standard Properties in the OAM11gRequest.xml File

Before you can register the Webgate agent with Oracle Access Manager, you must update some required properties in the `OAM11gRequest.xml` file.

---

**Note:**

If you plan to use the default values for most of the parameters in the provided XML file, then you can use the shorter version (`OAM11gRequest_short.xml`, in which all non-listed fields will take a default value.

---

---

**Note:** In the primary server list, the default names are mentioned as OAM_SERVER1 and OAM_SERVER2 for OAM servers. Rename these names in the list if the server names are changed in your environment.

---

To perform this task:

1. If you are using in-band mode, then change directory to the following location in the directory:

   *OAM_ORACLE_HOME*/oam/server/rreg/input

   If you are using out-of-band mode, then change directory to the location where you unpacked the RREG archive.

2. Make a copy of the `OAM11GRequest.xml` file template.

3. Review the properties listed in the file, and then update your copy of the OAM11GRequest.xml file to make sure the properties reference the host names and other values specific to your environment.

| OAM11gRequest.xml Property | Set to... |
|---|---|
| `serverAddress` | The host and the port of the Administration Server for the Oracle Access Manager domain. |
| `agentName` | Any custom name for the agent. Typically, you use a name that identifies the Fusion Middleware product you are configuring for single sign-on. |
| `applicationDomain` | A value that identifies the Web tier host and the FMW component you are configuring for single sign-on. |
| `security` | The security mode of the Oracle Access Manager server, which can be open, simple, or certificate mode.<br>For an enterprise deployment, Oracle recommends simple mode, unless additional requirements exist to implement custom security certificates for the encryption of authentication and authorization traffic.<br>In most cases, avoid using open mode, because in open mode, traffic to and from the Oracle Access Manager server is not encrypted.<br>For more information using certificate mode or about Oracle Access Manager supported security modes in general, see Securing Communication Between OAM Servers and WebGates in the *Administrator's Guide for Oracle Access Management*. |
| `cachePragmaHeader` | private |
| `cacheControlHeader` | private |
| `ipValidation` | 0<br>`<ipValidation>0<ipValidation>` |
| `ipValidationExceptions` | The IP address of the front-end load balancer. For example:<br>`<ipValidationExceptions>`<br>`  <ipAddress>130.35.165.42</ipAddress>`<br>`</ipValidation>` |
| `agentBaseUrl` | The host and the port of the machine on which Oracle HTTP Server 12*c* WebGate is installed. |

## 19.5.3 Updating the Protected, Public, and Excluded Resources for an Enterprise Deployment

When you set up an Oracle Fusion Middleware environment for single sign-on, you identify a set of URLs that you want Oracle Access Manager to protect with single sign-on. You identify these using specific sections of the `OAM11gRequest.xml` file. To identify the URLs:

1. If you haven't already opened `OAM11GRequest.xml` file for editing, locate and open the file in a text editor.

   For more information, see the following:

- Updating the Standard Properties in the OAM11gRequest.xml File

2. Remove the sample entries from the file, and then enter the list of protected, public, and excluded resources in the appropriate sections of the file, as shown in the following example.

---

**Note:**

If you are using Oracle Access Manager 11*g* Release 2 (11.1.2.2) or later, then note that the entries with the wildcard syntax ("`.../*`") are included in this example for backward compatibility with previous versions of Oracle Access Manager.

---

```
<protectedResourcesList>
 <!-- FMW/WLS Common Infrastruture Protected Resources-->
      <resource>/console/.../*</resource>
      <resource>/console</resource>
      <resource>/em/.../*</resource>
      <resource>/em</resource>
 <!-- WebCenter Portal Protected Resources -->
      <resource>/owc_discussions/admin/.../*</resource>
      <resource>/owc_discussions/login!default.jspa</resource>
      <resource>/owc_discussions/login!withredirect.jspa</resource>
      <resource>/owc_discussions/login.jspa</resource>
      <resource>/pagelets/admin/.../*</resource>
      <resource>/rest/api</resource>
      <resource>/rest/api/activities/.../*</resource>
      <resource>/rest/api/activities</resource>
      <resource>/rest/api/catalog/.../*</resource>
      <resource>/rest/api/catalog</resource>
      <resource>/rest/api/cmis/.../*</resource>
      <resource>/rest/api/cmis/</resource>
      <resource>/rest/api/discussions/.../*</resource>
      <resource>/rest/api/discussions</resource>
      <resource>/rest/api/feedback/.../*</resource>
      <resource>/rest/api/feedback</resource>
      <resource>/rest/api/messageBoards/.../*</resource>
      <resource>/rest/api/messageBoards</resource>
      <resource>/rest/api/navigations/.../*</resource>
      <resource>/rest/api/navigations</resource>
      <resource>/rest/api/people/.../*</resource>
      <resource>/rest/api/people</resource>
      <resource>/rest/api/preferences/general/.../*</resource>
      <resource>/rest/api/preferences/general</resource>
      <resource>/rest/api/resourceIndex</resource>
      <resource>/rest/api/searchcollection/.../*</resource>
      <resource>/rest/api/searchcollection</resource>
      <resource>/rest/api/searchresults/.../*</resource>
      <resource>/rest/api/searchresults</resource>
      <resource>/rest/api/spaces/.../*</resource>
      <resource>/rest/api/spaces</resource>
      <resource>/rest/api/taggeditems/.../*</resource>
      <resource>/rest/api/taggeditems</resource>
      <resource>/rest/api/taggingusers/.../*</resource>
      <resource>/rest/api/taggingusers</resource>
      <resource>/rest/api/tags/.../*</resource>
      <resource>/rest/api/tags</resource>
      <resource>/rest/api/v1/resourceIndex</resource>
      <resource>/rest/api/who/.../*</resource>
```

```
      <resource>/rest/api/who</resource>
      <resource>/rsscrawl/.../*</resource>
      <resource>/rsscrawl</resource>
      <resource>/rss/rssservlet</resource>
      <resource>/services-producer/adfAuthentication</resource>
      <resource>/sesUserAuth/.../*</resource>
      <resource>/sesUserAuth</resource>
      <resource>/webcenter/adfAuthentication</resource>
 <!-- WebCenter Content Protected Resources -->
      <resource>/adfAuthentication</resource>
      <resource>/cs/groups/.../*</resource>
      <resource>/cs/groups</resource>
      <resource>/cs/idcplg/.../*</resource>
      <resource>/cs/idcplg</resource>
      <resource>/dc-client/adfAuthentication</resource>
      <resource>/dc-console/adfAuthentication</resource>
      <resource>/ibr/adfAuthentication</resource>
      <resource>/imaging/faces/.../*</resource>
      <resource>/imaging/faces</resource>
      <resource>/wcc/adfAuthentication</resource>
<!-- SOA Protected Resources -->
      <resource>/DefaultToDoTaskFlow/.../*</resource>
      <resource>/DefaultToDoTaskFlow</resource>
      <resource>/EssHealthCheck/.../*</resource>
      <resource>/EssHealthCheck</resource>
      <resource>/b2bconsole/.../*</resource>
      <resource>/b2bconsole</resource>
      <resource>/ess/.../*</resource>
      <resource>/ess</resource>
      <resource>/inspection.wsil</resource>
      <resource>/integration/worklistapp/.../*</resource>
      <resource>/integration/worklistapp</resource>
      <resource>/sdpmessaging/userprefs-ui/.../*</resource>
      <resource>/sdpmessaging/userprefs-ui</resource>
      <resource>/soa-/composer/.../*</resource>
      <resource>/soa/composer/.../*</resource>
      <resource>/soa/composer</resource>
      <resource>/soa/composer</resource>
      <resource>/soa-infra/cluster/info/.../*</resource>
      <resource>/soa-infra/cluster/info</resource>
      <resource>/soa-infra/deployer/.../*</resource>
      <resource>/soa-infra/deployer</resource>
      <resource>/soa-infra/events/edn-db-log/.../*</resource>
      <resource>/soa-infra/events/edn-db-log</resource>
      <resource>/soa-infra</resource>
      <resource>/workflow/DefaultToDoTaskFlow/.../*</resource>
      <resource>/workflow/DefaultToDoTaskFlow</resource>
      <resource>/workflow/sdpmessagingsca-ui-worklist/.../*</resource>
      <resource>/workflow/sdpmessagingsca-ui-worklist</resource>
<!-- SOA Portal Taskflow Protected Resources --(For WCP/SOA integrated systems
only) -->
      <resource>/workflow/WebCenterWorklistDetail/faces/adf.task-flow/…/*</
resource>
      <resource>/workflow/WebCenterWorklistDetail/faces/adf.task-flow</resource>
</protectedResourcesList>
<publicResourcesList>
 <!-- WebCenter Portal Public Resources-->
      <resource>/owc_discussions/.../*</resource>
      <resource>/owc_discussions</resource>
      <resource>/pagelets</resource>
      <resource>/pagelets/welcome</resource>
```

```
      <resource>/rss/.../*</resource>
      <resource>/rss</resource>
      <resource>/services-producer</resource>
      <resource>/webcenterhelp/.../*</resource>
      <resource>/webcenterhelp</resource>
      <resource>/webcenter/.../*</resource>
      <resource>/webcenter</resource>
      <resource>/webcenterhelp</resource>
      <resource>/wsrp-tools</resource>
 <!-- WebCenter Content Public Resources -->
      <resource>/_ocsh/.../*</resource>
      <resource>/_ocsh</resource>
      <resource>/_dav/.../*</resource>
      <resource>/_dav</resource>
      <resource>/cs/.../*</resource>
      <resource>/cs</resource>
      <resource>/dc-console/.../*</resource>
      <resource>/dc-console</resource>
      <resource>/ibr/.../*</resource>
      <resource>/ibr</resource>
      <resource>/imaging/.../*</resource>
      <resource>/imaging</resource>
      <resource>/wcc/.../*</resource>
      <resource>/wcc</resource>
<!-- SOA Public Resources --(For SOA systems only) -->
      <resource>/soa-infra/directWSDL</resource>
<!-- SOA Portal Taskflow Public Resources --(For WCP/SOA integrated systems only)
-->
      <resource>/workflow/WebCenterWorklistDetail/…/*</resource>
      <resource>/workflow/WebCenterWorklistDetail</resource>
</publicResourcesList>
<excludedResourcesList>
      <resource>/favicon.ico</resource>
 <!-- FMW/WLS Common Infrastruture Excluded Resources -->
      <resource>/wsm-pm/.../*</resource>
      <resource>/wsm-pm</resource>
 <!-- WebCenter Portal Excluded Resources-->
      <resource>/collector/.../*</resource>
      <resource>/collector</resource>
      <resource>/owc_discussions/OWCDiscussionsServiceAuthenticated</resource>
      <resource>/owc_discussions/OWCDiscussionsServiceAuthenticated/.../*</
resource>
      <resource>/owc_discussions/OWCDiscussionsServicePublic</resource>
      <resource>/owc_discussions/OWCDiscussionsServicePublic/.../*</resource>
      <resource>/pagelets/api/v2/ensemble/pagelets</resource>
      <resource>/pagelets/api/v2/ensemble/pagelets/.../*</resource>
      <resource>/pagelets/ensemblestatic/.../*</resource>
      <resource>/pagelets/ensemblestatic</resource>
      <resource>/portalTools/.../*</resource>
      <resource>/portalTools</resource>
      <resource>/rsscrawl</resource>
      <resource>/rsscrawl/.../*</resource>
      <resource>/sesUserAuth</resource>
      <resource>/sesUserAuth/.../*</resource>
      <resource>/webcenter/SpacesWebService</resource>
      <resource>/webcenter/SpacesWebService/.../*</resource>
      <resource>/wsrp-tools/portlets/.../*</resource>
      <resource>/wsrp-tools/portlets</resource>
 <!-- WebCenter Content Excluded Resources -->
      <resource>/cs/common/idcapplet.jar</resource>
      <resource>/cs/images/.../*</resource>
```

```
      <resource>/cs/images</resource>
      <resource>/idcnativews/.../*</resource>
      <resource>/idcnativews</resource>
<!-- SOA Portal Taskflow Excluded Resources --(For WCP/SOA integrated systems
only) -->
      <resource>/soa-infra/services/default/CommunityWorkflows/**</resource>
      <resource>/soa-infra/services/default/CommunityWorkflows*</resource>
<!-- SOA Excluded Resources --(For SOA systems only) -->
      <resource>/soa-infra/services/.../*</resource>
      <resource>/ucs/messaging/webservice</resource>
      <resource>/ucs/messaging/webservice/.../*</resource>
      <resource>/integration/services/.../*</resource>
      <resource>/integration/services</resource>
      <resource>/b2b/services/</resource>
      <resource>/b2b/services/.../*</resource>
</excludedResourcesList>
```

3. Save and close the `OAM11GRequest.xml` file.

## 19.5.4 Running the RREG Tool

The following topics provide information about running the RREG tool to register your Oracle HTTP Server Webgate with Oracle Access Manager.

Running the RREG Tool in In-Band Mode

Running the RREG Tool in Out-Of-Band Mode

### 19.5.4.1 Running the RREG Tool in In-Band Mode

To run the RREG Tool in in-band mode:

1. Navigate to the RREG home directory.

   If you are using in-band mode, the RREG directory is inside the Oracle Access Manager Oracle home:

   *RREG_HOME*/oam/server/rreg

   If you are using out-of-band mode, then the RREG home directory is the location where you unpacked the RREG archive.

2. In the RREG home directory, navigate to the bin directory:

   ```
   cd RREG_HOME/bin/
   ```

3. Set the permissions of the `oamreg.sh` command so you can execute the file:

   ```
   chmod +x oamreg.sh
   ```

4. Run the following command:

   ```
   ./oamreg.sh inband input/OAM11GRequest.xml
   ```

In this example:

- It is assumed the edited `OAM11GRequest.xml` file is located in the *RREG_HOME*`/input` directory.
- The output from this command will be saved to the following directory:

  *RREG_HOME*/output/

The following example shows a sample RREG session:

```
Welcome to OAM Remote Registration Tool!
Parameters passed to the registration tool are:
Mode: inband
Filename: /u01/oracle/products/fmw/iam_home/oam/server/rreg/client/rreg/input/
OAM11GWCCDomainRequest.xml
Enter admin username:weblogic_idm
Username: weblogic_idm
Enter admin password:
Do you want to enter a Webgate password?(y/n):
n
Do you want to import an URIs file?(y/n):
n

---------------------------------------
Request summary:
OAM11G Agent Name:WCC1221_EDG_AGENT
URL String:null
Registering in Mode:inband
Your registration request is being sent to the Admin server at: http://
host1.example.com:7001
---------------------------------------

Jul 08, 2015 7:18:13 PM oracle.security.jps.util.JpsUtil disableAudit
INFO: JpsUtil: isAuditDisabled set to true
Jul 08, 2015 7:18:14 PM oracle.security.jps.util.JpsUtil disableAudit
INFO: JpsUtil: isAuditDisabled set to true
Inband registration process completed successfully! Output artifacts are created in
the output folder.
```

#### 19.5.4.2 Running the RREG Tool in Out-Of-Band Mode

To run the RREG Tool in out-of-band mode on the WEBHOST server, the administrator uses the following command:

```
RREG_HOME/bin/oamreg.sh outofband input/OAM11GRequest.xml
```

In this example:

- Replace *RREG_HOME* with the location where the RREG archive file was unpacked on the server.
- The edited `OAM11GRequest.xml` file is located in the *`RREG_HOME`*`/input` directory.
- The RREG Tool saves the output from this command (the *`AgentID`*`_response.xml` file) to the following directory:

  ```
  RREG_HOME/output/
  ```

  The Oracle Access Manager server administrator can then send the *`AgentID`*`_response.xml` to the user who provided the `OAM11GRequest.xml` file.

To run the RREG Tool in out-of-band mode on the Web server client machine, use the following command:

```
RREG_HOME/bin/oamreg.sh outofband input/AgentID_response.xml
```

In this example:

- Replace *RREG_HOME* with the location where you unpacked the RREG archive file on the client system.
- The *AgentID*_response.xml file, which was provided by the Oracle Access Manager server administrator, is located in the *RREG_HOME*/input directory.
- The RREG Tool saves the output from this command (the artifacts and files required to register the Webgate software) to the following directory on the client machine:

  *RREG_HOME*/output/

## 19.5.5 Files and Artifacts Generated by RREG

The files that get generated by the RREG Tool vary, depending on the security level you are using for communications between the WebGate and the Oracle Access Manager server. For more information about the supported security levels, see Securing Communication Between OAM Servers and WebGates in *Administrator's Guide for Oracle Access Management*.

Note that in this topic any references to *RREG_HOME* should be replaced with the path to the directory where you ran the RREG tool. This is typically the following directory on the Oracle Access Manager server, or (if you are using out-of-band mode) the directory where you unpacked the RREG archive:

*OAM_ORACLE_HOME*/oam/server/rreg/client

The following table lists the artifacts that are always generated by the RREG Tool, regardless of the Oracle Access Manager security level.

| File | Location |
|---|---|
| cwallet.sso | *RREG_HOME*/output/Agent_ID/ |
| ObAccessClient.xml | *RREG_HOME*/output/Agent_ID/ |

The following table lists the additional files that are created if you are using the SIMPLE or CERT security level for Oracle Access Manager:

| File | Location |
|---|---|
| aaa_key.pem | *RREG_HOME*/output/Agent_ID/ |
| aaa_cert.pem | *RREG_HOME*/output/Agent_ID/ |
| password.xml | *RREG_HOME*/output/Agent_ID/ |

Note that the password.xml file contains the obfuscated global passphrase to encrypt the private key used in SSL. This passphrase can be different than the passphrase used on the server.

You can use the files generated by RREG to generate a certificate request and get it signed by a third-party Certification Authority. To install an existing certificate, you must use the existing aaa_cert.pem and aaa_chain.pem files along with password.xml and aaa_key.pem.

### 19.5.6 Copying Generated Artifacts to the Oracle HTTP Server WebGate Instance Location

After the RREG Tool generates the required artifacts, manually copy the artifacts from the *RREG_Home*/output/*agent_ID* directory to the Oracle HTTP Server configuration directory on the Web tier host.

The location of the files in the Oracle HTTP Server configuration directory depends upon the Oracle Access Manager security mode setting (OPEN, SIMPLE, or CERT).

The following table lists the required location of each generated artifact in the Oracle HTTP Server configuration directory, based on the security mode setting for Oracle Access Manager. In some cases, you might have to create the directories if they do not exist already. For example, the wallet directory might not exist in the configuration directory.

---

**Note:**

For an enterprise deployment, Oracle recommends simple mode, unless additional requirements exist to implement custom security certificates for the encryption of authentication and authorization traffic. The information about using open or certification mode is provided here as a convenience.

Avoid using open mode, because in open mode, traffic to and from the Oracle Access Manager server is not encrypted.

For more information using certificate mode or about Oracle Access Manager supported security modes in general, see Securing Communication Between OAM Servers and WebGates in *Administrator's Guide for Oracle Access Management*.

---

| File | Location When Using OPEN Mode | Location When Using SIMPLE Mode | Location When Using CERT Mode |
|---|---|---|---|
| wallet/cwallet.sso | *OHS_CONFIG_DIR*/webgate/config/wallet | *OHS_CONFIG_DIR*/webgate/config/wallet/ | *OHS_CONFIG_DIR*/webgate/config/wallet/ |

**Note:**

By default the wallet folder is not available

| File | Location When Using OPEN Mode | Location When Using SIMPLE Mode | Location When Using CERT Mode |
|---|---|---|---|
| | | | le. Create the wallet folder under *OHS_CONFIG_DIR*/webga |

| File | Location When Using OPEN Mode | Location When Using SIMPLE Mode | Location When Using CERT Mode |
|---|---|---|---|
| | | | t e / c o n f i g / . |
| ObAccessClient.xml | *OHS_CONFIG_DIR*/ webgate/config | *OHS_CONFIG_DIR*/ webgate/config/ | *OHS_CONFIG_DIR*/ webgate/config/ |
| password.xml | N/A | *OHS_CONFIG_DIR*/ webgate/config/ | *OHS_CONFIG_DIR*/ webgate/config/ |
| aaa_key.pem | N/A | *OHS_CONFIG_DIR*/ webgate/config/ simple/ | *OHS_CONFIG_DIR*/ webgate/config/ |
| aaa_cert.pem | N/A | *OHS_CONFIG_DIR*/ webgate/config/ simple/ | *OHS_CONFIG_DIR*/ webgate/config/ |

**Note:** If you need to redeploy the `ObAccessClient.xml` to `WEBHOST1` and `WEBHOST2`, delete the cached copy of `ObAccessClient.xml` from the servers. The cache location on `WEBHOST1` is:

*OHS_DOMAIN_HOME*/servers/ohs1/cache/

And you must perform the similar step for the second Oracle HTTP Server instance on `WEBHOST2`:

*OHS_DOMAIN_HOME*/servers/ohs2/cache/

## 19.5.7 Restarting the Oracle HTTP Server Instance

For information about restarting the Oracle HTTP Server instance, see Restarting Oracle HTTP Server Instances by Using WLST in *Administrator's Guide for Oracle HTTP Server*.

If you have configured Oracle HTTP Server in a WebLogic Server domain, you can also use Oracle Fusion Middleware Control to restart the Oracle HTTP Server instances. For more information, see Restarting Oracle HTTP Server Instances by Using Fusion Middleware Control in *Administrator's Guide for Oracle HTTP Server*.

## 19.6 Setting Up the WebLogic Server Authentication Providers

To set up the WebLogic Server authentication providers, back up the configuration files, set up the Oracle Access Manager Identity Assertion Provider and set the order of providers.

The following topics assumes that you have already configured the LDAP authenticator by following the steps in Creating a New LDAP Authenticator and Provisioning Enterprise Deployment Users and Group. If you have not already created the LDAP authenticator, then do so before continuing with this section.



### 19.6.1 Backing Up Configuration Files

To be safe, 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
```

### 19.6.2 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. Click **Security Realms** in the left navigation bar.
4. Click the **myrealm** default realm entry.
5. Click the **Providers** tab.
6. Click **New**, and select the asserter type **OAMIdentityAsserter** from the drop-down menu.
7. Name the asserter (for example, *OAM ID Asserter*) and click **OK**.
8. Click the newly added asserter to see the configuration screen for the Oracle Access Manager identity assertion provider.
9. Set the control flag to *REQUIRED*.
10. Under Chosen types, select both the **ObSSOCookie** and **OAM_REMOTE_USER** options, if they are not selected by default.
11. Click **Save** to save the settings.

12. Click **Activate Changes** to propagate the changes.

### 19.6.3 Updating the Default Authenticator and Setting the Order of Providers

Set the order of identity assertion and authentication providers in the WebLogic Server Administration Console.

To update the default authenticator and 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. From the left navigation, select **Security Realms**.
4. Click the **myrealm** default realm entry.
5. Click the **Providers** tab.
6. From the table of providers, click the **DefaultAuthenticator**.
7. Set the Control Flag to `SUFFICIENT`.
8. Click **Save** to save the settings.
9. From the navigation breadcrumbs, click **Providers** to return to the list of providers.
10. Click **Reorder**.
11. Sort the providers to ensure that the OAM Identity Assertion provider is first and the DefaultAuthenticator provider is last.

***Table 19-1 Sort order***

| Sort Order | Provider | Control Flag |
|---|---|---|
| 1 | OAMIdentityAsserter | `REQUIRED` |
| 2 | LDAP Authentication Provider | `SUFFICIENT` |
| 3 | DefaultAuthenticator | `SUFFICIENT` |
| 4 | Trust Service Identity Asserter | `N/A` |
| 5 | DefaultIdentityAsserter | `N/A` |

12. Click **OK**.
13. Click **Activate Changes** to propagate the changes.
14. Restart the Administration Server, Managed Servers, and any system components, as applicable.

## 19.7 Configuring Oracle ADF and OPSS Security with Oracle Access Manager

Some Oracle Fusion Middleware management consoles use Oracle Application Development Framework (Oracle ADF) security, which can integrate with Oracle

Access Manager Single Sign On (SSO). These applications can take advantage of Oracle Platform Security Services (OPSS) SSO for user authentication, but you must first configure the domain-level `jps-config.xml` file to enable these capabilities.

The domain-level `jps-config.xml` file is located in the following location after you create an Oracle Fusion Middleware domain:

*DOMAIN_HOME*`/config/fmwconfig/jps-config.xml`

---

**Note:**

The domain-level `jps-config.xml` should not be confused with the `jps-config.xml` that is deployed with custom applications.

---

To update the OPSS configuration to delegate SSO actions in Oracle Access Manager, complete the following steps:

1. Change directory to the following directory:

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

2. Start the WebLogic Server Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server, using the following WLST command:

   ```
   connect('admin_user','admin_password','admin_url')
   ```

   For example:

   ```
   connect('weblogic_bi','mypassword','t3://ADMINVHN:7001')
   ```

4. Execute the `addOAMSSOProvider` command, as follows:

   ```
   addOAMSSOProvider(loginuri="/${app.context}/adfAuthentication", logouturi="/
   oamsso/logout.html")
   ```

   The following table defines the expected value for each argument in the addOAMSSOProvider command.

| Argument | Definition |
|---|---|
| loginuri | Specifies the URI of the login page<br><br>**Note:** For ADF security enabled applications, "/*context-root*/adfAuthentication" should be provided for the 'loginuri' parameter.<br><br>For example:<br><br>`/${app.context}/adfAuthentication`<br><br>**Note:** `${app.context}` must be entered as shown. At runtime, the application replaces the variable appropriately.<br><br>Here is the flow:<br><br>**a.** User accesses a resource that has been protected by authorization policies in OPSS, fox example.<br><br>**b.** If the user is not yet authenticated, ADF redirects the user to the URI configured in 'loginuri'.<br><br>**c.** Access Manager, should have a policy to protect the value in 'loginuri': for example, "/*context-root*/adfAuthentication".<br><br>**d.** When ADF redirects to this URI, Access Manager displays a Login Page (depending on the authentication scheme configured in Access Manager for this URI). |
| logouturi | Specifies the URI of the logout page<br>Notes:<br>• For ADF security enabled applications, `logouturi` should be configured based on logout guidelines in "Configuring Centralized Logout for Sessions Involving 11g WebGates" in the *Administrator's Guide for Oracle Access Management*.<br>• When using WebGate 11*g*, the value of the `logouturi` should be sought from the 11g WebGate Administrator.<br>• When using WebGate 10g, the value of `logouturi` should be `/oamsso/logout.html`. |
| autologinuri | Specifies the URI of the autologin page. This is an optional parameter. |

5. Disconnect from the Administration Server:

```
disconnect()
```

6. Restart the Administration Server and all the Managed Servers.

## 19.8 Additional Single Sign-on Configurations

The configurations described in the following sections may be necessary or helpful in providing additional security for your site.

Configuring WebCenter Portal for SSO

Configuring the Discussions Server for SSO

Configuring OAM Policies for WebCenter Portal REST Interfaces
The WebCenter Portal REST APIs need to be configured for a stateless basic authentication scheme in Oracle Access Manager.

Configuring OAM for RSS Feeds Using External Readers

Configuring the WebLogic Server Administration Console and Enterprise Manager for OAM 11g

Configuring Secure Enterprise Search for SSO

Configuring Content Server for SSO

Restricting Access with Connection Filters

Configuring Portlet Producers and Additional Components

### 19.8.1 Configuring WebCenter Portal for SSO

Configure the WebCenter Portal application for SSO by adding a setting to `EXTRA_JAVA_PROPERTIES`.

There is a system property that tells WebCenter Portal and ADF that the application is configured in SSO mode and some special handling is required. The following system property is required in this mode:

| Field | Value | Comment |
|---|---|---|
| `oracle.webcenter.spaces.osso` | `true` | This flag tells WebCenter Portal that SSO is being used, so no login form should be displayed on the default landing page. Instead, it displays a login link that the user can click to invoke the SSO authentication. |

To set this property:

1. Edit the `setUserOverrides.sh` script in the `ASERVER_HOME/bin` folder on WCPHOST1. Add the new java property name-value pair to the end of the existing EXTRA_JAVA_PROPERTIES variable value with an entry like the following:

```
EXTRA_JAVA_PROPERTIES="${EXTRA_JAVA_PROPERTIES} -
Doracle.webcenter.spaces.osso=true"
export EXTRA_JAVA_PROPERTIES
```

2. Copy this file to `MSERVER_HOME/bin` on WCPHOST1, WCPHOST2, WCCHOST1, and WCCHOST2.

3. Restart the Managed Servers in the Portal_Cluster from the WebLogic Server Console or WLST.

## 19.8.2 Configuring the Discussions Server for SSO

This section describes how to configure the discussions server for single sign-on.

---

**Note:**

Direct login to the discussions server is not supported after SSO is configured. Log in must be done through the Oracle HTTP Server URL.

---

To set up the discussions server for SSO:

1. Log in to the discussions server Admin Console at:

   `http://host:port/owc_discussions/admin`

   Where *`host`* and *`port`* are the host ID and port number of the `WC_Collaboration` managed server.

2. Open the System Properties page and edit (if it already exists) or add the `owc_discussions.sso.mode` property, setting it's value to `true`.

3. Edit or add the `jiveURL` property, setting the value to the front-end load-balancer public URL without including the protocol portion of the URL. For example:

   ```
   jiveURL = wcp.example.com/owc_discussions
   ```

   The `jiveURL` property is used when constructing links to forums in emails.

   ---

   **Note:**

   The registered WebCenter connection in WebCenter Portal for discussions and forums should point to the front-end load-balancer public URL.

   ---

4. Restart the Managed Servers in the Collab_Cluster from the WebLogic Server Console or WLST.

## 19.8.3 Configuring OAM Policies for WebCenter Portal REST Interfaces

The WebCenter Portal REST APIs need to be configured for a stateless basic authentication scheme in Oracle Access Manager.

To set up a new Authentication Scheme, complete the following steps:

1. Open the OAM Admin Console.

2. Navigate to your Application Domain's Authentication Policies view.

   For example, **Launch Pad** > **Access Manager Application Domains Link** > **search** > *your application domain* > **Authentication Policies** Tab.

3. Select the **Protected Resource Policy** authentication policy (not authorization).

4. Sort the list of resources by Resource URL and locate rows for the `/rest` resource URLs.
5. Individually, delete the association of each of the `/rest/...` related resources from the Protected Resource Policy.
6. Click **Apply** and close the Protected Resource Policy view tab.
7. Select the **Public Resource Policy** authentication policy (not authorization).
8. Sort the list of resources by Resource URL and locate rows for the `/rest/` resource URLs.
9. Individually, delete the association of each of the `/rest/...` related resources from the Public Resource Policy.
10. Click **Apply** and close the Public Resource Policy view tab.
11. On the Authentication Policies view, click **Create**.
12. Enter the following attribute values:

***Table 19-2 Attribute values***

| Attribute | Value |
|---|---|
| Name | WebCenter REST Policy |
| Description | Protected, Basic Sessionless Authentication scheme that protects access to some URIs. |
| Authentication Scheme | BasicSessionlessScheme |
| Success URL | *<empty>* |
| Failure URL | *<empty>* |

13. On the Resources tab, Click **Add**.
14. In the Add Resources dialog box, search for a Resource URL of: `/rest`.
15. Select all the returned rows starting with `/rest`, then click **Add Selected**.

> **Note:** Use the shift key to select a range of rows, and be sure to scroll if required to select the complete list.

16. Confirm that the resources selected in the previous step appear in the resources table for the new WebCenter REST Policy.
17. Click **Apply**. Do not configure any responses or advanced rules.

## 19.8.4 Configuring OAM for RSS Feeds Using External Readers

By default, WebCenter Portal RSS feeds are protected by SSO. However, they will not work well with external readers if left protected. If access using external readers is important, Oracle recommends that the WebCenter Portal RSS resource be excluded from the OAM policy so that the authentication for the RSS Servlet is handled by WebLogic Server's BASIC authentication that external readers can handle.

Follow the steps below to unprotect RSS feed for OAM 11g:

1. Open the OAM Admin Console.
2. Navigate to your Application Domain's Resources view.

   For example,

   Launch Pad > Access Manager Application Domains Link > search > your application domain > Resources Tab
3. On the Resources view, use the search form filtering by a Resource type of HTP and a Resource URL of rss. .

   A result with the following resource URLs appears:

```
/rss/**
/rss*
/rss/.../*
/rss/rssservlet/**
/rss/rssservlet*
/rsscrawl/**
/rsscrawl*
/rsscrawl/.../*
```

   **Note:** Depending on the release of Oracle Access Manager in use, the syntax for these resource URLs may vary slightly.
4. For each resource, select the resource row and click **Edit**.
5. Review and update the Protection Level assigned to each of these six resources. Resources that are currently `Protected` should be changed to `Excluded`.

   Public resources (e.g. /rss*) can be optionally be changed to `Excluded`, or left as `Public`.

   Note that the resource's authentication policy and authorization policy are removed if the Protection Level is set to `Excluded`.

   **Note:** A protection level of `Public` provides Oracle Access Manager audit logging of requests for user-facing public service endpoints that are either unauthenticated or require authentication models other than user-facing SSO. The audit-only transaction for public resources includes additional workload imposed on the system for requests that are not authenticated or authorized by Oracle Access Manager. The additional workload for auditing public resource requests will be dependent on request rates and the capacity of your infrastructure. Use of the `Excluded` protection level avoids this overhead as requests to excluded resources are not logged or reported by Oracle Access Manager.

## 19.8.5 Configuring the WebLogic Server Administration Console and Enterprise Manager for OAM 11g

This section describes how to optionally set up OAM 11g single sign-on for the WebLogic Server Administration Console and Enterprise Manager.

**Notes::**

- Setting up OAM SSO for Enterprise Manager and the WebLogic Server Administration Console would provide single sign-on access to same set of users for whom OAM SSO access has been configured. If you want the web tier to be accessible to external users through OAM, but want administrators to log in directly to Enterprise Manager and the WebLogic Server Administration Console, then you may not want to complete this additional configuration step.
- The OAM policy resource protections may have been completed in the Updating the Protected, Public, and Excluded Resources for an Enterprise Deployment section earlier in this chapter. Note that the rewrite rule for admin SSO logout should still be completed. If you want to reverse that configuration, follow the steps in this section and change the protection level from Protected to Public.

To set up OAM 11g SSO for the WebLogic Server Administration Console and Enterprise Manager:

1. Log in to the OAM Console using your browser:

   `http://host:port/oamconsole`

2. From the Launch Pad, select the **Application Domains** link found in the **Access Manager** block.

   The Policy Manager pane displays.

3. Locate the application domain you created using the name while registering webgate agent.

4. Expand the Resources node and click **Create**.

   The Resource page displays.

5. Add the resources that must be secured. For each resource:

   a. Select `http` as the **Resource Type**.

   b. Select the **Host Identifier** created while registering the WebGate agent.

   c. Enter the **Resource URL** for the WebLogic Server Administration Console (`/console`) or Enterprise Manager (`/em`).

   d. Enter a **Description** for the resource and click **Apply**.

   e. Set the **Protection Level** to `Protected`.

6. Go to **Authentication Policies > Protected Resource Policy** and add the newly created resource.

7. Do the same under **Authorization Policies > Protected Resource Policy**>

8. On WEBHOST1 and WEBHOST2, update the `admin_vh.conf` file and add a RewriteRule to enable SSO logout for the WLS Console.

```
<VirtualHost WEBHOST1:7777>
 ServerName admin.example.com:80
```

```
 ServerAdmin you@your.address
 RewriteEngine On
 RewriteOptions inherit

 # SSO logout redirection for WLS Console
 RewriteRule ^/console/jsp/common/logout.jsp "/oamsso/logout.html?end_url=/
console" [R]

</VirtualHost>
```

9. Restart the Oracle HTTP Server for your changes to take effect.

   You should now be able to access the WebLogic Server Administration Console and Enterprise Manager with the following links:

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

   and be prompted with the OAM SSO login form.

## 19.8.6 Configuring Secure Enterprise Search for SSO

The crawl sources that are defined to crawl WebCenter Portal data and repositories used by WebCenter Portal and the corresponding authentication end points defined in SES must be routed through the Web Tier Oracle HTTP Server ports so that they can be properly authenticated (the authentication method continues to be BASIC and realm jazn.com).

For information about configuring SES connections, see Setting Up Oracle SES Connections in *Administering Oracle WebCenter Portal*.

## 19.8.7 Configuring Content Server for SSO

Once SSO is functional, the portal connection to Content Server should be updated to set the web context root path. Setting this parameter tells the Document Library code that SSO is configured. Note that the `webContextRoot` value should not be set until after SSO has been set up and is functional.

1. Change directory to the following directory:

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

2. Start the WebLogic Server Scripting Tool (WLST):

   ```
   ./wlst.sh
   ```

3. Connect to the Administration Server, using the following WLST command:

   ```
   connect('admin_user','admin_password','admin_url')
   ```

   For example:

   ```
   connect('weblogic_wcp','mypassword','t3://ADMINVHN:7001')
   ```

4. List the available content server connections and identify the correct connection name to use in the next command.

   ```
   listContentServerConnections(appName='webcenter', server='WC_Portal1')
   ```

5. Set the `webContextRoot` value for the Portal's Content Server connection as follows, substituting the correct value for the `name` parameter.

```
setContentServerConnection(appName='webcenter', server='WC_Portal1',
name='nameFromStep4', webContextRoot='/cs')
```

6. Restart the Portal clustered managed servers from your WLST session:

```
shutdown('Portal_Cluster', 'Cluster', block='true', force='true')
start('Portal_Cluster', 'Cluster')
```

7. Exit WLST.

```
exit()
```

### 19.8.8 Restricting Access with Connection Filters

Follow the steps below to only allow users to access WebCenter Portal and associated components through the web tier OHS ports so that they can be properly authenticated.

1. Log in to the WebLogic Server Administration Console.
2. In the **Domain Structure** pane, select the domain you want to configure (for example, `webcenter`).
3. Open the **Security** tab and the **Filter** subtab.

   The **Security Filter Settings** pane displays.
4. Check **Connection Logger Enabled** to enable the logging of accepted messages.

   The Connection Logger logs successful connections and connection data in the server. You can use this information to debug problems relating to server connections.
5. In the **Connection Filter** field, specify the connection filter class to be used in the domain.
   - To configure the default connection filter, specify `weblogic.security.net.ConnectionFilterImpl`.
   - To configure a custom connection filter, specify the class that implements the network connection filter. Note that this class must also be present in the CLASSPATH for WebLogic Server.
6. In the Connection Filter Rules field, enter the syntax for the connection filter rules.

   **Note:** Make sure to add the IP/subnets for the following - web tier, load balancer, end user access point, and hosts that contain the rest of the domain managed servers. Else, you will encounter a 403 error when trying to access the Administration Server.

   For example:

```
<webtier IP>/0 * * allow
0.0.0.0/0  *  *  deny
```

   which says: allow all traffic coming from the local host and disallow all traffic from any other IP address. You should, of course, write the network filter(s) that are relevant to your environment. For more information about writing connection

filters, see Developing Custom Connection Filters in *Developing Applications with the WebLogic Security Service*.

7. Click **Save** and activate the changes.
8. Restart all the managed servers and the Administration server.
9. Verify that all direct traffic to the WebLogic Server is blocked by attempting to navigate to:

   ```
   http://wcp.example.com/webcenter
   ```

   This should produce the following error:

   ```
   "The Server is not able to service this request: [Socket:
   000445]Connection rejected, filter blocked Socket,
   weblogic.security.net.FilterException: [Security:090220]rule
   3"
   ```

   You should, however, still be able to access WebCenter Portal through the OHS port:

   ```
   http://wcp.example.com/webcenter
   ```

### 19.8.9 Configuring Portlet Producers and Additional Components

If you have set up your Portlet Producer applications to route through OHS, be sure to use the OHS host and port when specifying producer URLs for registration. This applies to out of-the-box producers like wsrp-tools, services-producer, pagelet producers and any other producer you have explicitly configured.

Be sure to use the internal load-balancer URL (for example, http://wcp-internal.example.com/...) when specifying producer URLs for registration. This applies to out of-the-box producers like wsrp-tools, services-producer, pagelet producers and any other producer you have explicitly configured.

# 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 provides information about multi data sources and Oracle RAC and procedure for configuring multi data sources for an Enterprise Deployment.



## A.1 About Multi Data Sources and Oracle RAC

A multi data source provides an ordered list of data sources to use to satisfy connection requests.

Normally, every connection request to this kind of multi data source is served by the first data source in the list. If a database connection test fails and the connection cannot be replaced, or if the data source is suspended, a connection is sought sequentially from the next data source on the list.

For more information about configuring Multi Data Sources with Oracle RAC, see "Using Multi Data Sources with Oracle RAC" in the *Oracle Fusion Middleware Configuring and Managing JDBC Data Sources for Oracle WebLogic Server*.

## A.2 Typical Procedure for Configuring Multi Data Sources for an Enterprise Deployment

You configure data sources when you configure a domain. If you want to use Multi Data Sources instead of GridLink data sources, replace the GridLink instructions with the instructions provided in this section.

For example, when you are configuring the initial Administration domain for an Enterprise Deployment reference topology, you use the configuration wizard to define the characteristics of the domain, as well as the data sources.

The procedures for configuring the topologies in this Enterprise Deployment Guide include specific instructions for defining GridLink data sources with Oracle RAC. If you want to use Multi Data Sources instead of GridLink data sources, replace the GridLink instructions with the following:

1. In the Configure JDBC Component Schema screen:

a. Select the appropriate schemas.

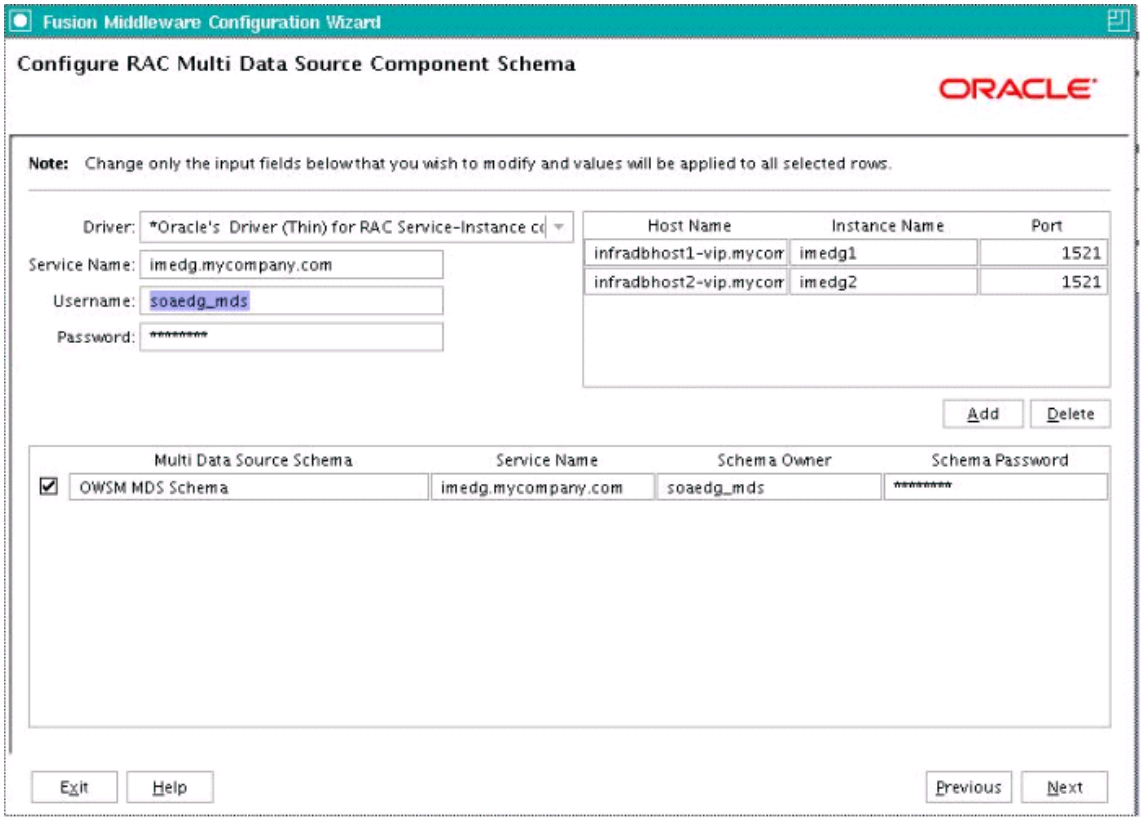
b. For the RAC configuration for component schemas, **Convert to RAC multi data source**.

c. Ensure that the following data source appears on the screen with the schema prefix when you ran the Repository Creation Utility.

d. Click **Next**.

2. The Configure RAC Multi Data Sources Component Schema screen appears (Figure A-1).

***Figure A-1 Configure RAC Multi Data Source Component Schema Screen***




In this screen, do the following:

a. Enter values for the following fields, specifying the connect information for the Oracle RAC database that was seeded with RCU.

- **Driver:** Select **Oracle driver (Thin) for RAC Service-Instance connections, Versions:10, 11**.
- **Service Name:** Enter the service name of the database.
- **Username:** Enter the complete user name (including the prefix) for the schemas.
- **Password:** Enter the password to use to access the schemas.

b. Enter the host name, instance name, and port.

c. Click **Add**.

d. Repeat this for each Oracle RAC instance.

e. Click **Next**.

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

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

# Index