

Oracle® Fusion Applications

Financials Enterprise Deployment Guide

11g Release 1 (11.1.4)

E27364-02

June 2012

Documentation for system administrators who are installing and configuring Oracle Fusion Applications components in an enterprise deployment for Oracle Fusion Financials.

Copyright © 2012 Oracle and/or its affiliates. All rights reserved.

Primary Authors: Karen Ram (Writer), Janga Aliminati (Architect), Sriramulu Lakkaraju, Susan Kornberg, Pramodini Gattu, Arulvenkatesh Mathuranayagamnagappan, Milan Parikh, Venu Surakanti

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

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

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

U.S. GOVERNMENT END USERS: Oracle programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, delivered to U.S. Government end users are "commercial computer software" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, use, duplication, disclosure, modification, and adaptation of the programs, including any operating system, integrated software, any programs installed on the hardware, and/or documentation, shall be subject to license terms and license restrictions applicable to the programs. No other rights are granted to the U.S. Government.

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

Oracle and Java are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Xeon are trademarks or registered trademarks of Intel Corporation. All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. AMD, Opteron, the AMD logo, and the AMD Opteron logo are trademarks or registered trademarks of Advanced Micro Devices. UNIX is a registered trademark of The Open Group.

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

Contents

Preface	xiii
Audience	xiii
Documentation Accessibility	xiii
Related Documents	xiii
Conventions	xiv
1 Enterprise Deployment Overview	
1.1 What is an Enterprise Deployment?	1-1
1.2 About Oracle Fusion Applications	1-2
1.3 Benefits of Oracle Recommendations	1-2
1.3.1 Built-in Security	1-3
1.3.2 High Availability	1-3
1.4 Terminology	1-3
2 Introduction to the Enterprise Deployment Reference Topologies	
2.1 Overview of Reference Enterprise Deployment Topologies	2-1
2.1.1 Overall Reference Enterprise Deployment Topology	2-1
2.1.2 Reference Topologies Documented in the Guide	2-3
2.1.2.1 Oracle Fusion Financials Domain	2-3
2.1.2.2 Oracle Fusion Customer Relationship Management Domain	2-4
2.1.2.3 Oracle Fusion Common Domain	2-5
2.1.2.4 Oracle Fusion Human Capital Management Domain	2-6
2.1.2.5 Oracle Fusion Supply Chain Management Domain	2-7
2.1.2.6 Oracle Fusion Projects Domain	2-8
2.1.2.7 Oracle Fusion Procurement Domain	2-9
2.1.2.8 Oracle Business Intelligence Domain	2-10
2.1.3 About the Web Tier Nodes	2-11
2.1.3.1 Load Balancer Requirements	2-12
2.1.4 About the Application Tier	2-13
2.1.5 About the Data Tier	2-13
2.2 Hardware Requirements	2-13
2.3 Installation Prerequisite	2-14
2.4 Implementing the Topology	2-14

3 Preparing the Network for an Enterprise Deployment

3.1	External Virtual Server Names	3-1
3.2	Internal Virtual IPs	3-2
3.3	Load Balancer Configuration	3-2
3.4	Reference Enterprise Deployment Directory Structure	3-3
3.4.1	Directory Structure	3-3
3.4.2	Binary Directory Structure	3-4
3.4.3	Domain Configuration Directory Structure	3-5
3.5	Shared Storage	3-5
3.5.1	Shared Storage for Oracle Business Intelligence	3-5
3.6	IPs and Virtual IPs	3-6
3.7	Firewalls and Ports	3-8
3.8	Clock Synchronization	3-12

4 Preparing the Database for an Enterprise Deployment

4.1	Understanding the Database in the Enterprise Deployment Topology	4-1
4.2	Setting Up the Database	4-2
4.2.1	Database Host Requirements	4-2
4.2.2	Supported Database Versions	4-2
4.2.3	Minimum Database Configuration Parameters	4-3
4.3	Creating and Starting the Database Services	4-5
4.3.1	Updating the Kernel Parameters	4-5
4.4	Loading the Oracle Fusion Applications Repository into the Oracle RAC Database	4-6
4.5	Backing Up the Database	4-12

5 Using the Provisioning Process to Install Components for an Enterprise Deployment

5.1	Understanding Provisioning	5-1
5.2	Prerequisites for Using the Provisioning Process	5-1
5.3	Installing Components	5-3
5.3.1	Creating the Installation Environment	5-3
5.3.1.1	Downloading the Provisioning Repository	5-3
5.3.1.2	Installing the Provisioning Framework Bits	5-3
5.3.1.2.1	Running the Provisioning Installer	5-4
5.3.2	Creating a New Provisioning Response File	5-5
5.3.2.1	Installation Options Screen	5-6
5.3.2.2	Specify Security Updates Screen	5-6
5.3.2.3	Provisioning Configurations Screen	5-6
5.3.2.4	Response File Description Screen	5-7
5.3.2.5	Installation Location Screen	5-7
5.3.2.6	System Port Allocation Screen	5-9
5.3.2.7	Database Configuration Screen	5-9
5.3.2.8	Schema Passwords Screen	5-10
5.3.2.9	ODI Password Configuration Screen	5-11
5.3.2.10	Domain Topology Configuration Screen	5-12
5.3.2.11	Web Tier Configuration Screen	5-13

5.3.2.12	Virtual Hosts Configuration Screen	5-14
5.3.2.13	Load Balancer Configuration Screen	5-15
5.3.2.14	Web Proxy Configuration Screen	5-16
5.3.2.15	Identity Management Configuration Screen	5-17
5.3.2.16	Access and Policy Management Configuration Screen	5-20
5.3.2.17	IDM Database Configuration Screen	5-22
5.3.2.18	Summary Screen	5-23
5.3.3	Running the Provisioning Commands to Install Components	5-23
5.4	Configuring Components	5-26
5.5	Performing Post-Provisioning Tasks	5-30
5.5.1	Validation	5-30
5.5.2	Other Tasks	5-30
6	Scaling Out Oracle HTTP Server	
6.1	Performing the Scaleout	6-1
6.2	Performing WebGate Post-Installation Steps	6-16
6.3	Installing WebGate Patches	6-18
6.4	Wiring Oracle HTTP Server with Load Balancer	6-18
6.5	Validating Oracle HTTP Server on WEBHOST2	6-18
7	Setting Up Node Manager for an Enterprise Deployment	
7.1	Setting Up Node Manager for FINHOST2	7-1
7.2	Creating the Identity Keystore on FINHOST2	7-2
8	Scaling Out the Oracle Fusion Financials Domain	
8.1	Overview of the Oracle Fusion Financials Domain	8-1
8.2	Prerequisites for Scaling Out the Oracle Fusion Financials Domain	8-1
8.3	Adding a New Machine in the Oracle WebLogic Server Console	8-2
8.4	Packing and Unpacking the Managed Server Domain Home	8-2
8.5	Cloning Managed Servers and Assigning Them to FINHOST2	8-3
8.6	Oracle HTTP Server Configuration	8-5
8.7	Configuring Server Migration for the Managed Servers	8-6
8.8	Validating the System	8-6
9	Scaling Out the Oracle Fusion Customer Relationship Management Domain	
9.1	Overview of the Oracle Fusion Customer Relationship Management Domain	9-1
9.2	Prerequisites for Scaling Out the Oracle Fusion Customer Relationship Management Domain	9-2
9.3	Adding a New Machine in the Oracle WebLogic Server Console	9-2
9.4	Packing and Unpacking the Managed Server Domain Home	9-3
9.5	Cloning Managed Servers and Assigning Them to FINHOST2	9-3
9.6	Oracle HTTP Server Configuration	9-6
9.7	Configuring Server Migration for the Managed Servers	9-6
9.8	Validating the System	9-7

10 Scaling Out the Oracle Fusion Common Domain

10.1	Overview of the Oracle Fusion Common Domain	10-1
10.2	Prerequisites for Scaling Out the Oracle Fusion Common Domain	10-2
10.3	Adding a New Machine in the Oracle WebLogic Server Console	10-2
10.4	Scaling Out Oracle WebCenter Content	10-3
10.4.1	Creating a Common Location for the WebCenter Content Managed Servers	10-3
10.4.2	Configuring Oracle WebCenter Content: Imaging	10-3
10.4.2.1	Prerequisite	10-4
10.4.2.2	Configuring the WebCenter Content Server	10-4
10.4.2.3	Configuring a JMS Persistence Store	10-5
10.4.2.4	Configuring a Default Persistence Store for Transaction Recovery	10-5
10.4.2.5	Adding the Oracle Imaging Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content	10-6
10.4.2.6	Creating a Connection to Oracle WebCenter Content	10-7
10.5	Packing and Unpacking the Managed Server Domain Home	10-7
10.6	Cloning Managed Servers and Assigning Them to FINHOST2	10-8
10.7	Oracle HTTP Server Configuration	10-11
10.8	Configuring Server Migration for the Managed Servers	10-11
10.9	Validating the System	10-12

11 Scaling Out the Oracle Fusion Human Capital Management Domain

11.1	Overview of the Oracle Fusion Human Capital Management Domain	11-1
11.2	Prerequisites for Scaling Out the Oracle Fusion Human Capital Management Domain	11-1
11.3	Adding a New Machine in the Oracle WebLogic Server Console	11-2
11.4	Packing and Unpacking the Managed Server Domain Home	11-2
11.5	Cloning Managed Servers and Assigning Them to FINHOST2	11-3
11.6	Oracle HTTP Server Configuration	11-6
11.7	Configuring Server Migration for the Managed Servers	11-6
11.8	Validating the System	11-6

12 Scaling Out the Oracle Fusion Supply Chain Management Domain

12.1	Overview of the Oracle Fusion Supply Chain Management Domain	12-1
12.2	Prerequisites for Scaling Out the Oracle Fusion Supply Chain Management Domain	12-1
12.3	Adding a New Machine in the Oracle WebLogic Server Console	12-2
12.4	Packing and Unpacking the Managed Server Domain Home	12-2
12.5	Cloning Managed Servers and Assigning Them to FINHOST2	12-3
12.6	Oracle HTTP Server Configuration	12-5
12.7	Configuring Server Migration for the Managed Servers	12-6
12.8	Validating the System	12-6

13 Scaling Out the Oracle Fusion Projects Domain

13.1	Overview of the Oracle Fusion Projects Domain	13-1
13.2	Prerequisites for Scaling Out the Oracle Fusion Projects Domain	13-1
13.3	Adding a New Machine in the Oracle WebLogic Server Console	13-2
13.4	Packing and Unpacking the Managed Server Domain Home	13-2
13.5	Cloning Managed Servers and Assigning Them to FINHOST2	13-3

13.6	Oracle HTTP Server Configuration	13-6
13.7	Configuring Server Migration for the Managed Servers	13-6
13.8	Validating the System	13-7

14 Scaling Out the Oracle Fusion Procurement Domain

14.1	Overview of the Oracle Fusion Procurement Domain	14-1
14.2	Prerequisites for Scaling Out the Oracle Fusion Procurement Domain	14-2
14.3	Adding a New Machine in the Oracle WebLogic Server Console	14-2
14.4	Packing and Unpacking the Managed Server Domain Home	14-3
14.5	Cloning Managed Servers and Assigning Them to FINHOST2	14-3
14.6	Oracle HTTP Server Configuration	14-6
14.7	Configuring Server Migration for the Managed Servers	14-6
14.8	Validating the System	14-7

15 Scaling Out the Oracle Business Intelligence Domain

15.1	Overview of the Oracle Business Intelligence Domain	15-1
15.2	Prerequisites for Scaling Out the Oracle Business Intelligence Domain	15-2
15.3	Starting the Default Node Manager	15-3
15.4	Prerequisites for Scaling Out Oracle Business Intelligence on FINHOST2	15-3
15.4.1	Configuring JMS for Oracle BI Publisher	15-3
15.4.2	Setting the Listen Address for bi_server1 Managed Server	15-4
15.4.3	Updating the FusionVirtualHost_bi.conf Configuration File	15-5
15.5	Scaling Out Oracle Business Intelligence Components	15-7
15.5.1	Scaling Out the Oracle Business Intelligence System on FINHOST2	15-8
15.5.2	Starting Node Manager in SSL Mode	15-9
15.5.3	Scaling Out the System Components	15-10
15.5.4	Configuring Secondary Instances of Singleton System Components	15-11
15.5.5	Configuring the bi_server2 Managed Server	15-11
15.5.5.1	Setting the Listen Address for the bi_server2 Managed Server	15-12
15.5.5.2	Configuring Custom Identity and Custom Trust for the bi_server2 Managed Server	15-12
15.5.5.3	Disabling Host Name Verification for the bi_server2 Managed Server	15-13
15.5.5.4	Adding bi_server2 System Properties to the Server Start Tab	15-14
15.5.6	Performing Additional Configuration for Oracle Business Intelligence High Availability	15-15
15.5.6.1	Additional Configuration Tasks for Oracle BI Scheduler	15-15
15.5.6.2	Additional Configuration Tasks for Oracle Real-Time Decisions	15-16
15.5.6.2.1	Configuring Oracle Real-Time Decisions Clustering Properties	15-16
15.5.6.2.2	Adding Oracle RTD System Properties to the Server Start Tab	15-17
15.5.6.3	Additional Configuration Tasks for Oracle BI Publisher	15-18
15.5.6.3.1	Configuring Integration with Oracle BI Presentation Services	15-18
15.5.6.3.2	Setting the Oracle BI EE Data Source	15-19
15.5.6.3.3	Configuring JMS for BI Publisher	15-20
15.5.6.4	Additional Configuration Tasks for Oracle BI for Microsoft Office	15-21
15.5.6.4.1	Configuring Oracle BI for Microsoft Office Properties	15-21
15.5.6.4.2	Validating Oracle BI for Microsoft Office	15-22

15.5.6.5	Additional Configuration Tasks for Oracle Financial Reporting	15-24
15.5.7	Configuring a Default Persistence Store for Transaction Recovery	15-24
15.5.8	Starting and Validating Oracle Business Intelligence on FINHOST2	15-25
15.5.8.1	Starting the bi_server2 Managed Server	15-26
15.5.8.2	Starting the Oracle Business Intelligence System Components	15-26
15.5.8.3	Validating Oracle Business Intelligence URLs	15-26
15.5.9	Validating Access Through Oracle HTTP Server	15-27
15.5.10	Configuring Node Manager for the Managed Servers	15-27
15.5.11	Configuring Server Migration for the Managed Servers	15-28
15.6	Configuring Oracle Essbase Clustering	15-28
15.6.1	Validating Essbase Clustering	15-29
15.7	Validating the System	15-29

16 Additional Configuration Procedures for Scaling Out Oracle SOA Suite Server

16.1	Enabling Virtual IPs on FINHOST1 and FINHOST2	16-2
16.2	Setting the Listen Address for soa_server1	16-2
16.3	Setting the Listen Address for soa_server2	16-3
16.4	Updating the FusionVirtualHost_fin.conf Configuration File	16-3
16.5	Configuring JMS for the Oracle SOA Suite Server	16-4
16.6	Configuring Oracle Coherence for Deploying Composites	16-5
16.7	Configuring a Default Persistence Store for Transaction Recovery	16-7
16.8	Disabling Host Name Verification for the soa_server <i>n</i> Managed Servers	16-8
16.9	Restarting Node Manager on FINHOST1	16-9
16.10	Starting and Validating soa_server1 on FINHOST1	16-9
16.11	Restarting Node Manager on FINHOST2	16-9
16.12	Starting and Validating soa_server2 on FINHOST2	16-10

17 Configuring Administration Server High Availability

17.1	Enabling Administration Server High Availability	17-1
17.1.1	Enabling Administrative Virtual Host on FINHOST1	17-2
17.1.2	Adding a New Machine in the Oracle WebLogic Server Console	17-3
17.1.3	Enabling the Administration Server to Listen on the Virtual IP Address	17-3
17.2	Oracle HTTP Server Configuration	17-4
17.3	Validating the Administration Server	17-5
17.4	Manually Failing Over the Administration Server to FINHOST2	17-5
17.4.1	Prerequisites	17-5
17.4.2	Performing the Failover	17-5
17.5	Failing the Administration Server Back to FINHOST1	17-6

18 Setting Up Server Migration for an Enterprise Deployment

18.1	Prerequisite	18-1
18.2	Migrating Oracle Fusion Applications Domains	18-1
18.2.1	About Configuring Server Migration	18-1
18.2.2	Setting Up a User and Tablespace for the Server Migration Leasing Table	18-2

18.2.3	Creating a Multi-Data Source Using the Oracle WebLogic Server Administration Console	18-3
18.2.4	Editing Node Manager's Properties File	18-4
18.2.5	Setting Environment and Superuser Privileges for the wlsifconfig.sh Script	18-5
18.2.6	Configuring Server Migration Targets	18-6
18.2.7	Testing the Server Migration	18-7

19 Configuring Oracle Business Intelligence Applications

19.1	Introduction to Oracle BI Applications for Oracle Fusion Financials	19-1
19.1.1	Topology	19-2
19.2	Preparing for an Oracle BI Applications Installation	19-3
19.2.1	Creating Databases for Oracle Business Intelligence Applications Components	19-4
19.2.2	Running Oracle BI Applications RCU to Create the Oracle BI Applications Schemas for the Data Warehouse	19-4
19.2.3	Installing and Configuring Informatica PowerCenter Services	19-8
19.2.4	Extending the Oracle Business Intelligence Domain by Deploying Oracle BI Applications Configuration Manager, Functional Setup Manager, and DAC	19-8
19.2.4.1	How to Configure DAC, Oracle BI Applications Configuration Manager, and Functional Setup Manager	19-8
19.2.4.2	Configuring Data Warehouse Administration Console for High Availability	19-12
19.3	Performing Additional Configuration Tasks	19-12
19.4	Configuring Oracle HTTP Server for the Managed Server	19-12
19.5	Performing Additional Data Warehouse Administration Console Tasks	19-13
19.6	Validating Oracle BI Applications Components URLs	19-14

20 Managing the Topology

20.1	Scaling the Topology for Additional Nodes	20-1
20.1.1	Scaling Out the Topology (Adding Managed Servers to a New Node) for Oracle ADF Server	20-2
20.1.1.1	Prerequisites for Scaling Out the Topology for Oracle ADF Server	20-2
20.1.1.2	Adding a New Machine in the Oracle WebLogic Server Console	20-2
20.1.1.3	Packing and Unpacking the Managed Server Domain Home	20-3
20.1.1.4	Cloning Managed Servers and Assigning Them to FINHOST3	20-3
20.1.1.5	Validating the System	20-6
20.1.2	Scaling Up the Topology (Adding Managed Servers to an Existing Node) for Oracle ADF Server	20-6
20.1.2.1	Cloning Managed Servers and Assigning Them to FINHOST3	20-6
20.1.2.2	Validating the System	20-8
20.1.3	Scaling Out the Topology (Adding Managed Servers to a New Node) for Oracle SOA Suite Server	20-8
20.1.3.1	Prerequisites for Scaling Out the Topology for Oracle SOA Suite Server	20-9
20.1.3.2	Adding a New Machine in the Oracle WebLogic Server Console	20-9
20.1.3.3	Packing and Unpacking the Managed Server Domain Home	20-10
20.1.3.4	Cloning Managed Servers and Assigning Them to FINHOST3	20-10
20.1.3.5	Validating the System	20-13
20.1.3.6	Additional Configuration Procedures for Scaling Out Oracle SOA Suite Server	20-13

20.1.3.6.1	Enabling Virtual IPs on FINHOST3	20-13
20.1.3.6.2	Setting the Listen Address for soa_server3	20-14
20.1.3.6.3	Updating the FusionVirtualHost_fin.conf Configuration File	20-14
20.1.3.6.4	Configuring JMS for the Oracle SOA Suite Server	20-14
20.1.3.6.5	Configuring Oracle Coherence for Deploying Composites	20-15
20.1.3.6.6	Disabling Host Name Verification for the soa_server <i>n</i> Managed Servers	20-18
20.1.3.6.7	Restarting Node Manager on FINHOST3	20-18
20.1.3.6.8	Starting and Validating soa_server3 on FINHOST3	20-18
20.1.4	Scaling Up the Topology (Adding Managed Servers to an Existing Node) for Oracle SOA Suite Server	20-18
20.1.4.1	Cloning Managed Servers and Assigning Them to FINHOST3	20-18
20.1.4.2	Validating the System	20-19
20.1.5	Scaling Out the Topology (Adding Managed Servers to a New Node) for Oracle Business Intelligence	20-20
20.1.5.1	Prerequisites for Scaling Out the Topology for Oracle Business Intelligence ..	20-20
20.1.5.2	Scale-Out Procedure for Oracle Business Intelligence	20-21
20.1.6	Scaling Up the Topology for Oracle Business Intelligence	20-23
20.1.6.1	Scale-Up Procedure for Oracle Business Intelligence	20-23
20.2	Performing Backups and Recoveries	20-23
20.3	Monitoring the Topology	20-24
20.4	Migrating from a Test Environment to a Production Environment	20-24
20.5	Configuring Log File Rotation	20-24
20.5.1	Specifying Log File Rotation Using Oracle Enterprise Manager	20-25
20.5.2	Specifying Log File Rotation Using WLST	20-26
20.6	Patching the Topology	20-26
20.7	Auditing	20-26
20.8	Troubleshooting	20-28
20.8.1	Page Not Found When Accessing soa-infra Application Through Load Balancer ..	20-29
20.8.2	soa-infra Application Fails to Start Due to Deployment Framework Issues (Coherence)	20-29
20.8.3	Incomplete Policy Migration After Failed Restart of SOA Server	20-30
20.8.4	Oracle SOA Suite Server Fails to Start Due to Maximum Number of Processes Available in Database	20-31
20.8.5	Administration Server Fails to Start After a Manual Failover	20-31
20.8.6	Error While Activating Changes in Administration Console	20-31
20.8.7	SOA Server Not Failed Over After Server Migration	20-32
20.8.8	SOA Server Not Reachable From Browser After Server Migration	20-32
20.8.9	Oracle Access Manager Configuration Tool Does Not Remove URLs	20-32
20.8.10	Redirecting of Users to Login Screen After Activating Changes in Administration Console	20-33
20.8.11	Redirecting of Users to Administration Console's Home Page After Activating Changes to OAM	20-33
20.8.12	Configured JOC Port Already in Use	20-33
20.8.13	Out-of-Memory Issues on Managed Servers	20-33
20.8.14	JDBC Connection Reset Appears When on OEL 5.4	20-34
20.8.15	Missing JMS Instances on Oracle BI Publisher Scheduler Diagnostics Page	20-34
20.8.16	Oracle BI Publisher Jobs in Inconsistent State After Managed Server Shutdown ..	20-34
20.8.17	JMS Instance Fails in an Oracle BI Publisher Cluster	20-35

20.8.18	Administration Console Redirects from Internal URL to Container URL after Activation	20-35
---------	---	-------

A Deploying Administrative Clients for Oracle Fusion Applications

A.1	Recommended Solution	A-1
A.2	Implementation	A-3

Preface

This preface describes the audience, contents and conventions used in the *Oracle Fusion Applications Financials Enterprise Deployment Guide*.

Audience

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

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following documents in the Oracle Fusion Applications documentation set or in the Oracle Fusion Middleware documentation set:

- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence*
- *Oracle Fusion Middleware Configuration Guide for Oracle Business Intelligence Applications*
- *Oracle Fusion Applications Administrator's Guide*
- *Oracle Database Administrator's Guide*
- *Oracle Fusion Applications Installation Guide*
- *Oracle Fusion Middleware Repository Creation Utility User's Guide*
- *Oracle Real Application Clusters Administration and Deployment Guide*
- *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition)*

Conventions

The following text conventions are used in this document:

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

Enterprise Deployment Overview

This chapter provides an overview of the enterprise topology for Oracle Fusion Financials.

This chapter includes the following topics:

- [Section 1.1, "What is an Enterprise Deployment?"](#)
- [Section 1.2, "About Oracle Fusion Applications"](#)
- [Section 1.3, "Benefits of Oracle Recommendations"](#)
- [Section 1.4, "Terminology"](#)

1.1 What is an Enterprise Deployment?

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

An Oracle Fusion Applications enterprise deployment:

- considers various business Service Level Agreements (SLA) to make high-availability guidelines as widely applicable as possible
- leverages database grid servers and storage grid with low-cost storage to provide highly resilient, lower cost infrastructure
- uses results from extensive performance impact studies for different configurations to ensure that the high-availability architecture is optimally configured to perform and scale to business needs
- enables control over the length of time to recover from an outage and the amount of acceptable data loss from a natural disaster
- uses Oracle guidelines and recommended architecture, which are independent of hardware and operating systems.

Note: This document focuses on enterprise deployments in Linux environments. Enterprise deployments can also be implemented in UNIX and Windows environments.

1.2 About Oracle Fusion Applications

Oracle Fusion Applications are a unified suite of business applications designed to unify personal and enterprise processes. It unifies transactional Oracle SOA Suite and business processes, business intelligence, and collaborative technologies in a seamless user experience. Oracle Fusion Applications can be easily integrated into a service-oriented architecture and made available as software as a service.

Oracle Fusion Applications offer a strong functional value by providing:

- Installed based demand (for example, unified global payroll module)
- Competitive differentiation (for example, Distributed Order Orchestration)
- Revenue generation (for example, sales territory management)

Oracle Fusion Applications incorporate best practice business processes, including those from Oracle E-Business Suite, PeopleSoft, Oracle On Demand, JD Edwards, and Siebel.

Oracle Fusion Applications are standards-based, making them highly adaptable. This standards-based technology allows you to respond effectively to change with flexible, modular, user-driven business software that is powered by best-in-class business capabilities built on open standards. Its technology framework includes the following products:

- Oracle WebCenter Portal provides design time and runtime tools for building enterprise portals, transactional websites, and social networking sites.
- Oracle Business Intelligence 11g provides a full range of business intelligence capabilities that allow you to collect, present, and deliver organizational data.
- Hyperion extends Oracle's business intelligence capabilities to offer the most comprehensive system for enterprise performance management.
- Oracle WebCenter Content enables you to leverage document management, Web content management, digital asset management, and records retention functionality to build and complement your business applications.
- Oracle SOA Suite provides an enterprise architecture that supports building connected enterprise applications to provide solutions to business problems.
- Oracle WebLogic Server is a scalable, enterprise-ready Java Platform, Enterprise Edition (Java EE) application server.
- Oracle JDeveloper is an integrated development environment with end-to-end support for modeling, developing, debugging, optimizing, and deploying Java applications and Web services.
- Oracle Enterprise Manager Fusion Middleware Control offers business-driven applications management, integrated application to disk management, and integrated systems management and support experience.
- Oracle Identity Management enables organizations to manage the end-to-end life cycle of user identities and to secure access to enterprise resources and assets.

For more information, see the *Oracle Fusion Applications Concepts Guide*.

1.3 Benefits of Oracle Recommendations

The Oracle Fusion Applications configurations discussed in this guide are designed to ensure security of all invocations, maximize hardware resources, and provide a

reliable, standards-compliant system for enterprise computing with a variety of applications.

- [Built-in Security](#)
- [High Availability](#)

The security and high-availability benefits of the Oracle Fusion Applications configurations are realized through isolation in firewall zones and replication of software components.

1.3.1 Built-in Security

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

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

Note: The Oracle Technology Network (<http://www.oracle.com/technetwork/index.html>) provides a list of validated load balancers.

- Communication from external clients does not go beyond the Load Balancing Router (LBR) level.
- Components are separated in different protection zones: the Oracle Web Tier, application tier, and the data tier. Moreover, Oracle Identity Management (IDM) has its own protection zones like Oracle Web Tier, Applications tier and Data tier
- No direct communication from the Load Balancing Router to the data tier is allowed.
- Direct communication between two firewalls at any one time is prohibited.
- If a communication begins in one firewall zone, it must end in the next firewall zone.
- Oracle Internet Directory (OID) is isolated in the data tier.
- All communication between components across protection zones is restricted by port and protocol, according to firewall rules.

1.3.2 High Availability

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

1.4 Terminology

The following terminology is used in this enterprise deployment guide:

- **Oracle home:** An Oracle home contains installed files necessary to host a specific product. For example, the SOA Oracle home contains a directory that contains binary and library files for Oracle SOA Suite. An Oracle home resides within the

directory structure of the Middleware home. Each Oracle home can be associated with multiple Oracle instances or Oracle WebLogic Server domains.

- **ORACLE_BASE:** An alternate way of specifying the path `/u01/oracle`. Stores binaries, configuration, and Oracle Inventory.
- **WebLogic Server home:** A WebLogic Server home contains installed files necessary to host a WebLogic Server. The WebLogic Server home directory is a peer of Oracle home directories and resides within the directory structure of the Middleware home.
- **Middleware home:** A Middleware home consists of the Oracle WebLogic Server home, and, optionally, one or more Oracle homes. A Middleware home can reside on a local file system or on a remote shared disk that is accessible through NFS.
- **Oracle instance:** An Oracle instance contains one or more active middleware system components, for example Oracle Web Cache, Oracle HTTP Server or Oracle Internet Directory. You determine which components are part of an instance, either at install time or by creating and configuring an instance at a later time. An Oracle instance contains files that can be updated, such as configuration files, log files, temporary files.
- **Domain:** The basic administrative unit of Oracle WebLogic Server.
- **Managed Server:** Hosts business applications, application components, Web services, and their associated resources. To optimize performance, Managed Servers maintain a read-only copy of the domain's configuration document. When a Managed Server starts, it connects to the domain's Administration Server to synchronize its configuration document with the document that the Administration Server maintains.
- **failover:** When a member of a high availability system fails unexpectedly (unplanned downtime), in order to continue offering services to its consumers, the system undergoes a failover operation. If the system is an active-passive system, the passive member is activated during the failover operation and consumers are directed to it instead of the failed member. The failover process can be performed manually, or it can be automated by setting up hardware cluster services to detect failures and move cluster resources from the failed node to the standby node. If the system is an active-active system, the failover is performed by the load balancer entity serving requests to the active members. If an active member fails, the load balancer detects the failure and automatically redirects requests for the failed member to the surviving active members. See *Oracle Fusion Middleware High Availability Guide* for information on active-active and active-passive systems.
- **failback:** After a system undergoes a successful failover operation, the original failed member can be repaired over time and be re-introduced into the system as a standby member. If desired, a failback process can be initiated to activate this member and deactivate the other. This process reverts the system back to its pre-failure configuration.
- **hardware cluster:** A hardware cluster is a collection of computers that provides a single view of network services (for example: an IP address) or application services (for example: databases, Web servers) to clients of these services. Each node in a hardware cluster is a standalone server that runs its own processes. These processes can communicate with one another to form what looks like a single system that cooperatively provides applications, system resources, and data to users.

A hardware cluster achieves high availability and scalability through the use of specialized hardware (cluster interconnect, shared storage) and software (health

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

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

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

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

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

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

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

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

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

A load balancer also uses a virtual IP as the entry point to a set of servers. These servers tend to be active at the same time. This virtual IP address is not assigned to any individual server but to the load balancer which acts as a proxy between servers and their clients.

Introduction to the Enterprise Deployment Reference Topologies

This chapter describes and illustrates the Oracle Fusion Financials enterprise deployment reference topologies described in this guide. The road map for installation and configuration directs you to the appropriate chapters for the tasks you need to perform. Use this chapter to help you plan your Oracle Fusion Financials enterprise deployment.

This chapter includes the following topics:

- [Section 2.1, "Overview of Reference Enterprise Deployment Topologies"](#)
- [Section 2.2, "Hardware Requirements"](#)
- [Section 2.3, "Installation Prerequisite"](#)
- [Section 2.4, "Implementing the Topology"](#)

2.1 Overview of Reference Enterprise Deployment Topologies

This section describes diagrams used in an Oracle Fusion Financials enterprise deployment. Use this section to plan your enterprise deployment topology.

This section includes the following topics:

- [Section 2.1.1, "Overall Reference Enterprise Deployment Topology"](#)
- [Section 2.1.2, "Reference Topologies Documented in the Guide"](#)
- [Section 2.1.3, "About the Web Tier Nodes"](#)
- [Section 2.1.4, "About the Application Tier"](#)
- [Section 2.1.5, "About the Data Tier"](#)

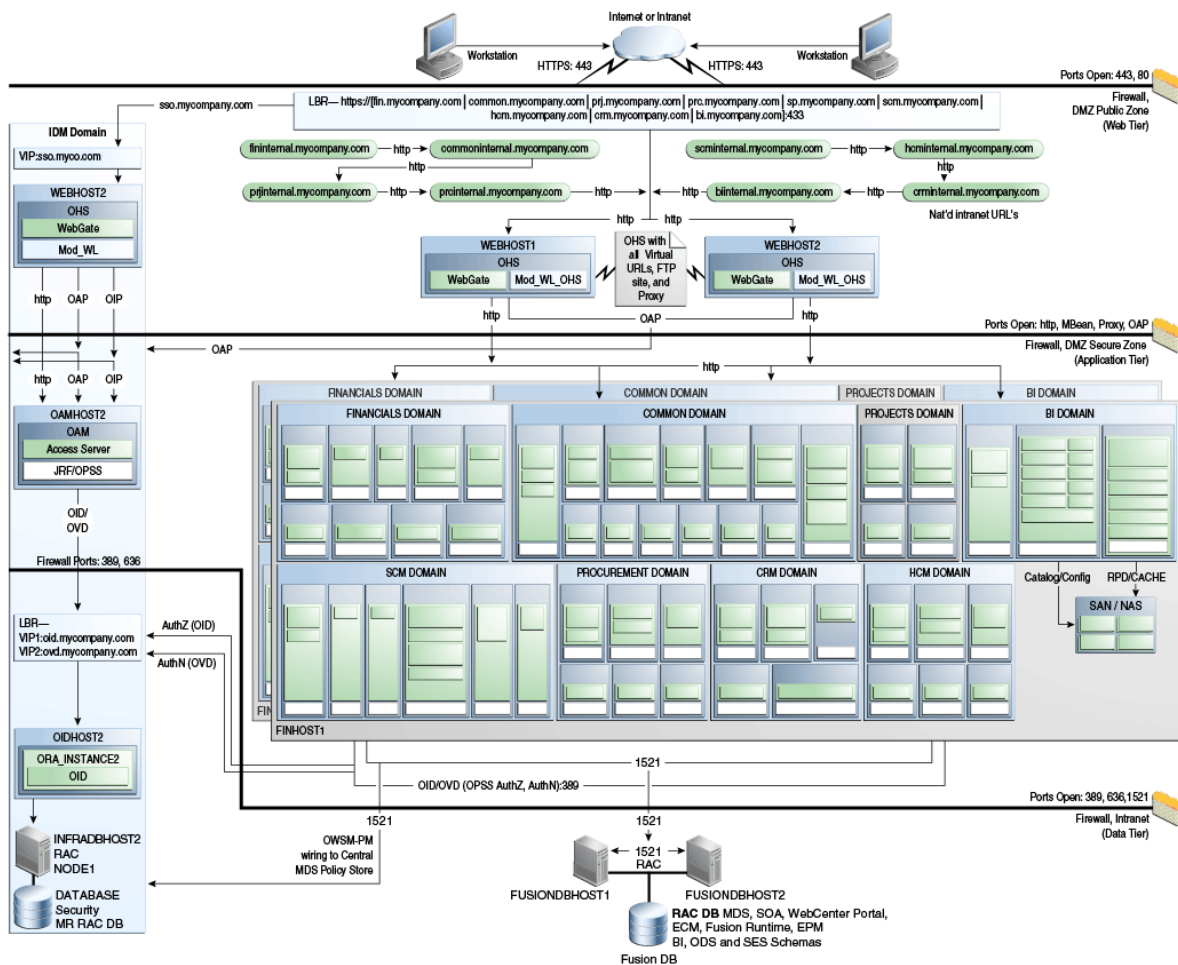
2.1.1 Overall Reference Enterprise Deployment Topology

[Figure 2–1](#) shows the overall Oracle Fusion Financials reference enterprise deployment topology, to which variations may be applied. The graphic illustrates how all components are deployed together.

In the topology, the primary node (also known as a host, and is *FINHOST* in the diagram) is actively running the Oracle Fusion Applications instance. The secondary node (*FINHOST2*) is the redundant (HA) node for the Oracle Fusion Applications instance. The primary node consists of an Administration Server and applications that have been deployed to Managed Servers. Managed Servers can be grouped together in

clusters to provide scalability and high availability for applications. Together, the primary and secondary nodes form a domain.

Figure 2–1 Oracle Fusion Financials Reference Enterprise Deployment Topology

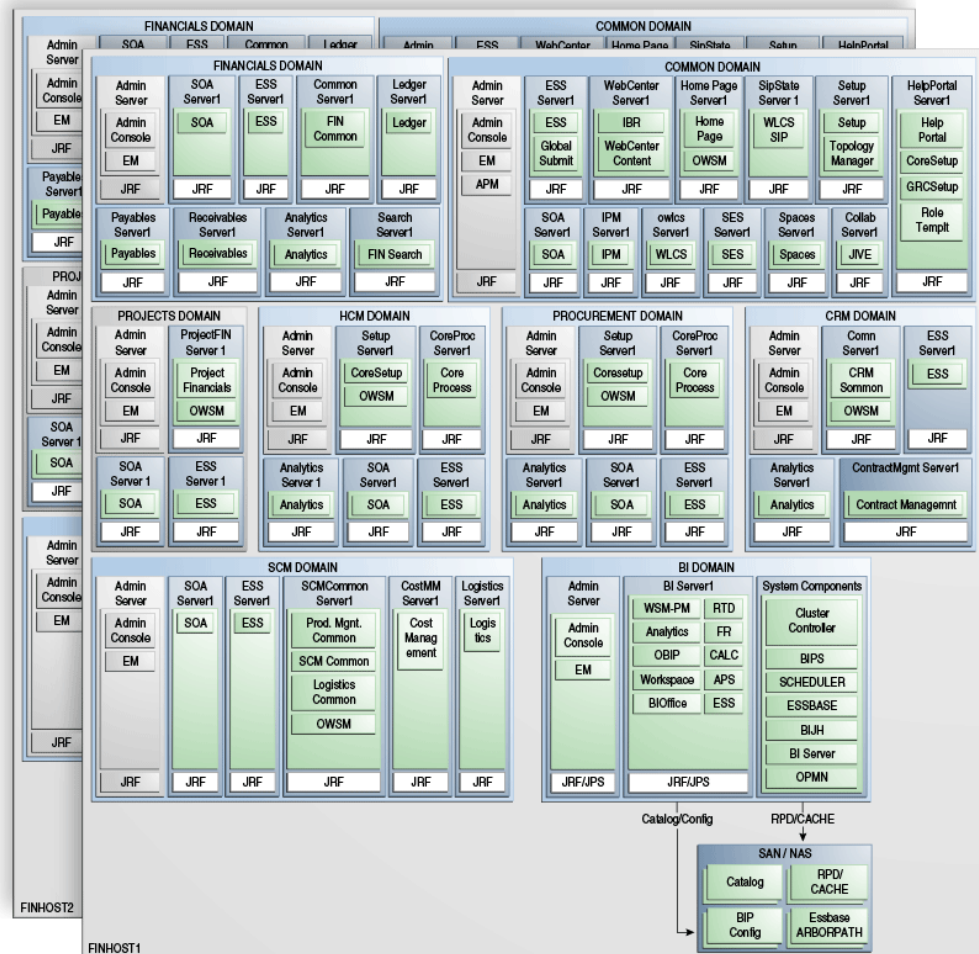


As shown in Figure 2–2, the overall Oracle Fusion Applications reference enterprise deployment topology comprises several domains:

- Oracle Fusion Financials Domain
- Oracle Fusion Customer Relationship Management Domain
- Oracle Fusion Common Domain
- Oracle Fusion Human Capital Management Domain
- Oracle Fusion Supply Chain Management Domain
- Oracle Fusion Projects Domain
- Oracle Fusion Procurement Domain
- Oracle Business Intelligence Domain

Figure 2–2 shows each of the domains in detail.

Figure 2-2 Domain Details



The scale out of these domains is described in the chapters that follow.

For information about installing the Oracle Identity Management stack for Oracle Fusion Applications, see [Section 5.2, "Prerequisites for Using the Provisioning Process."](#)

2.1.2 Reference Topologies Documented in the Guide

This section describes the references topologies used in an Oracle Fusion Financials enterprise deployment.

2.1.2.1 Oracle Fusion Financials Domain

Figure 2-3 shows the Oracle Fusion Financials domain within the overall reference enterprise deployment topology for Oracle Fusion Applications.

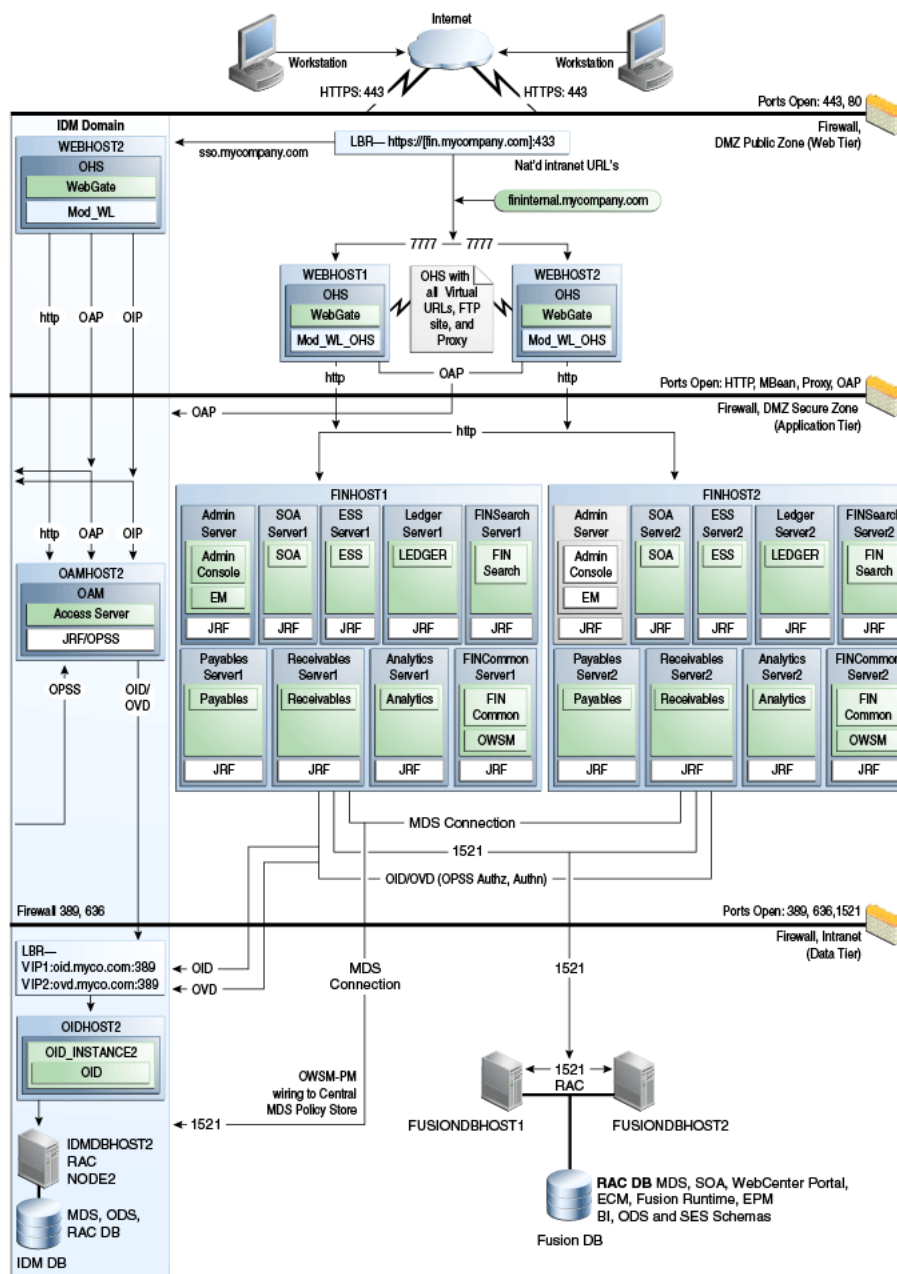
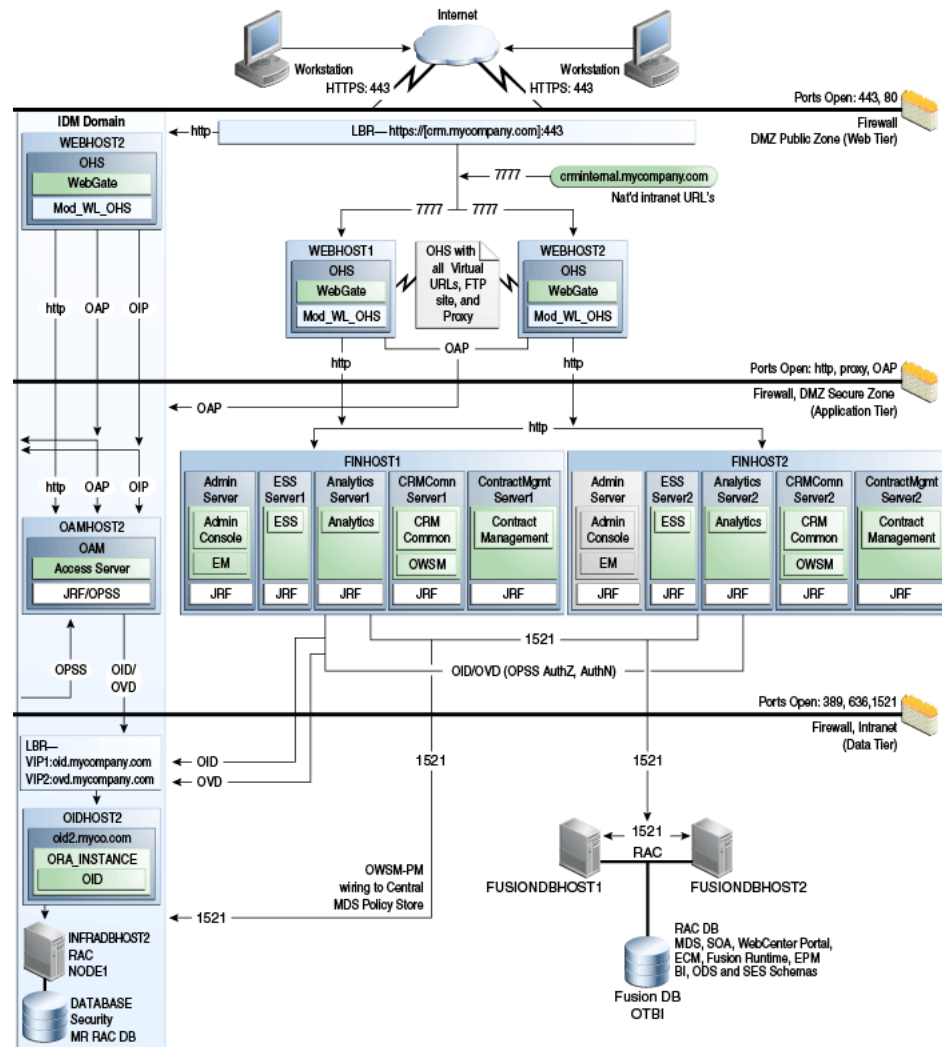
Figure 2-3 Reference Topology for Oracle Fusion Financials Domain**2.1.2.2 Oracle Fusion Customer Relationship Management Domain**

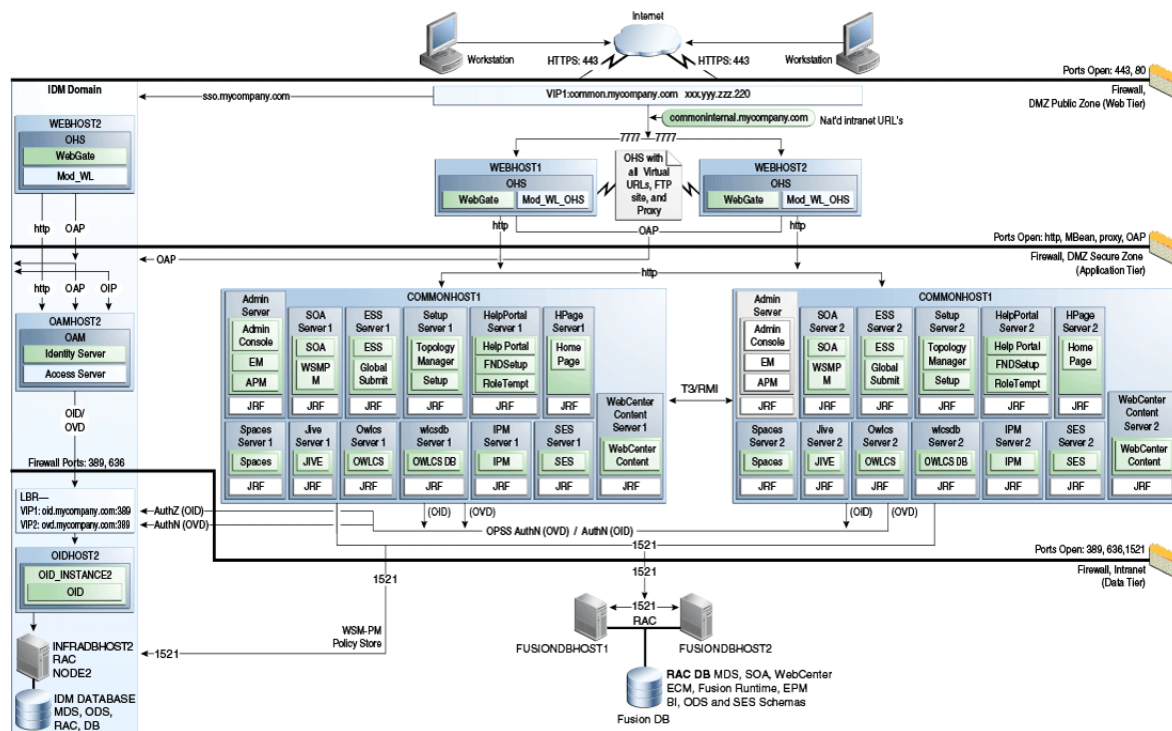
Figure 2-4 shows the Oracle Fusion Customer Relationship Management domain within the overall reference enterprise deployment topology for Oracle Fusion Applications.

Figure 2–4 Reference Topology for Oracle Fusion Customer Relationship Management Domain



2.1.2.3 Oracle Fusion Common Domain

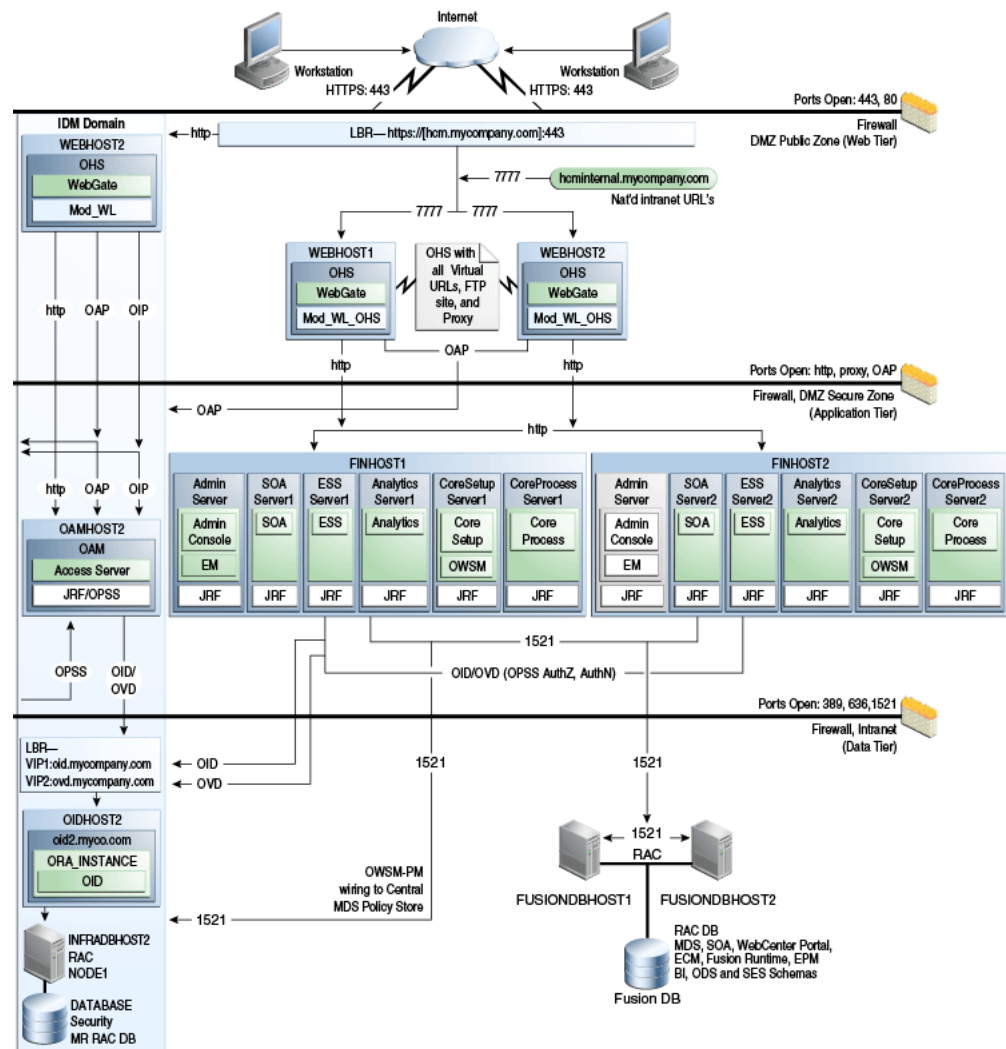
Figure 2–5 shows the Oracle Fusion Common domain within the overall reference enterprise deployment topology for Oracle Fusion Applications.

Figure 2–5 Reference Topology for Oracle Fusion Common Domain

2.1.2.4 Oracle Fusion Human Capital Management Domain

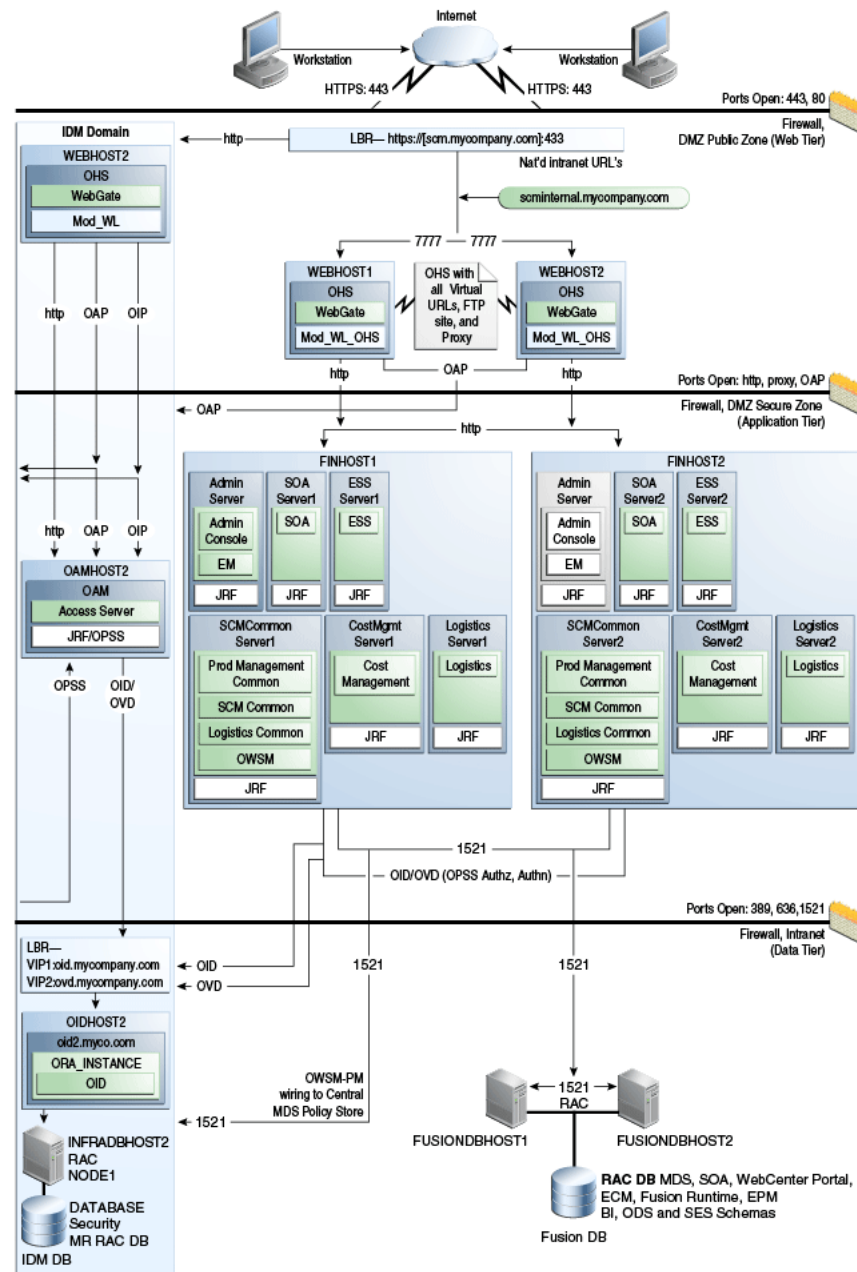
Figure 2–6 shows the Oracle Fusion Human Capital Management domain within the overall reference enterprise deployment topology for Oracle Fusion Applications.

Figure 2–6 Reference Topology for the Oracle Fusion Human Capital Management Domain



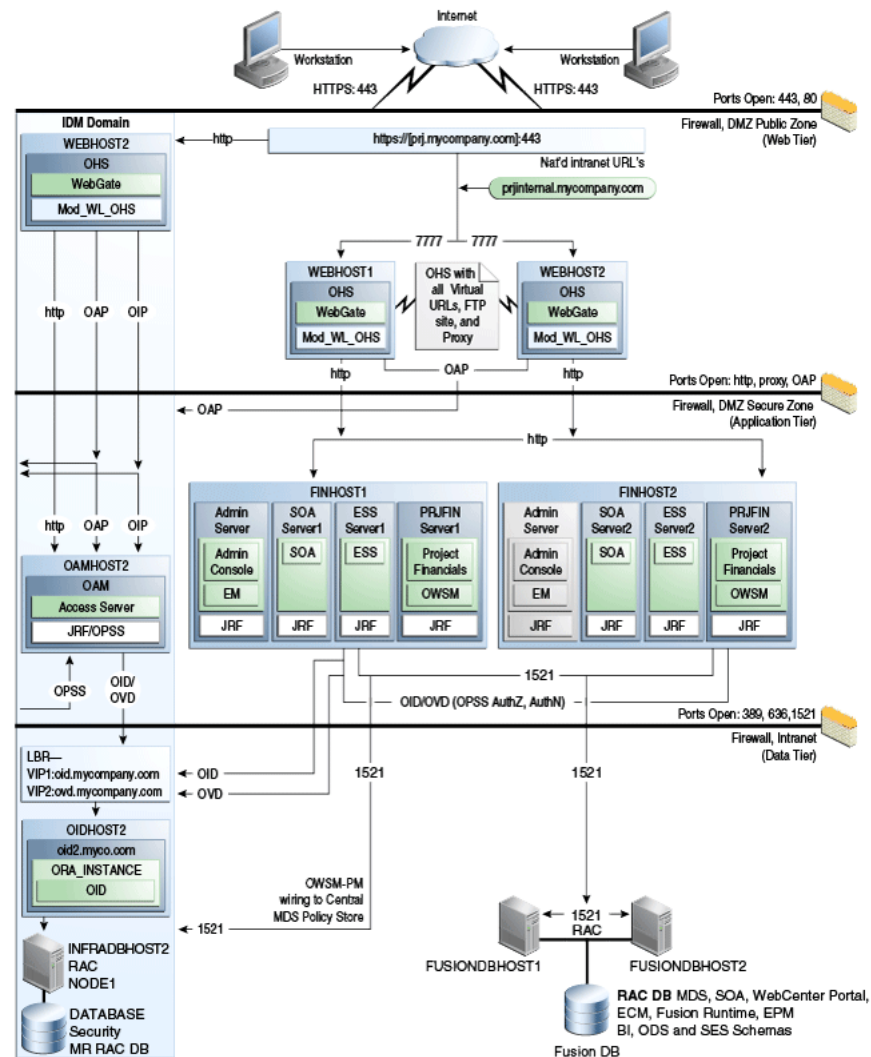
2.1.2.5 Oracle Fusion Supply Chain Management Domain

Figure 2–7 shows the Oracle Fusion Supply Chain Management domain within the overall reference enterprise deployment topology for Oracle Fusion Applications.

Figure 2–7 Reference Topology for Oracle Fusion Supply Chain Management Domain

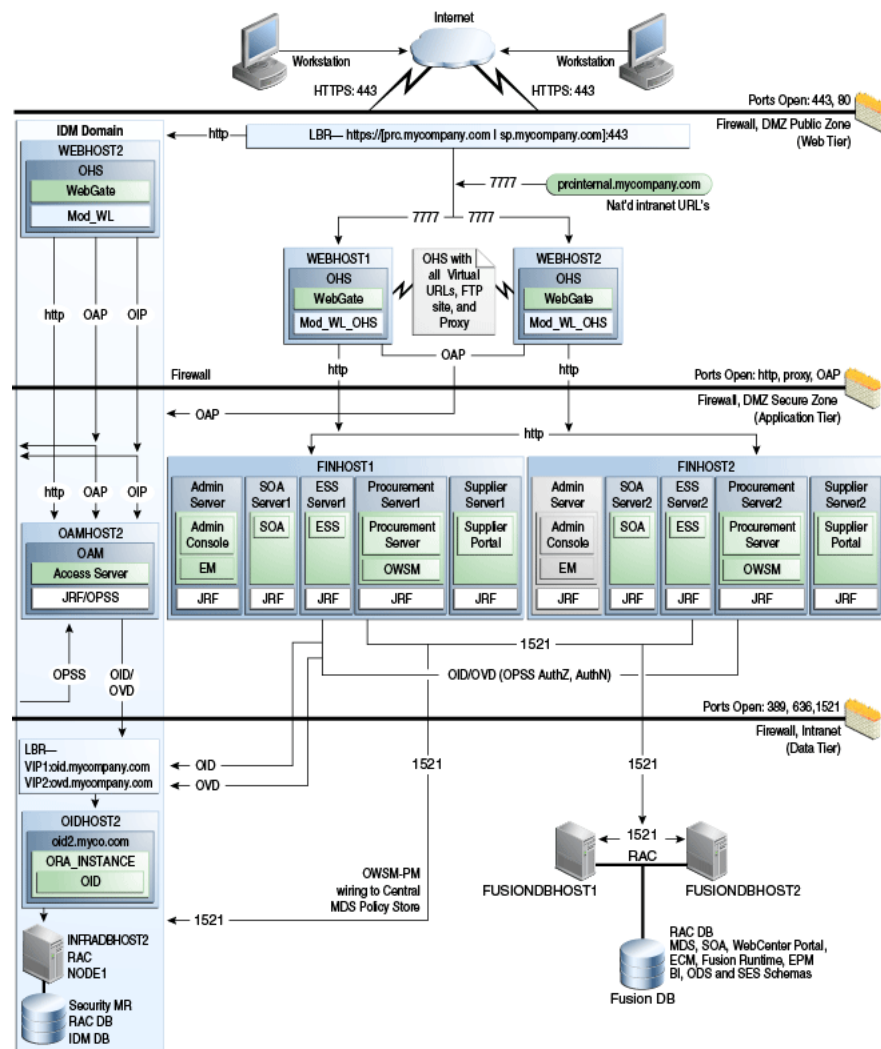
2.1.2.6 Oracle Fusion Projects Domain

Figure 2–8 shows the Oracle Fusion Projects domain within the overall reference enterprise deployment topology for Oracle Fusion Applications.

Figure 2–8 Reference Topology for Oracle Fusion Projects Domain

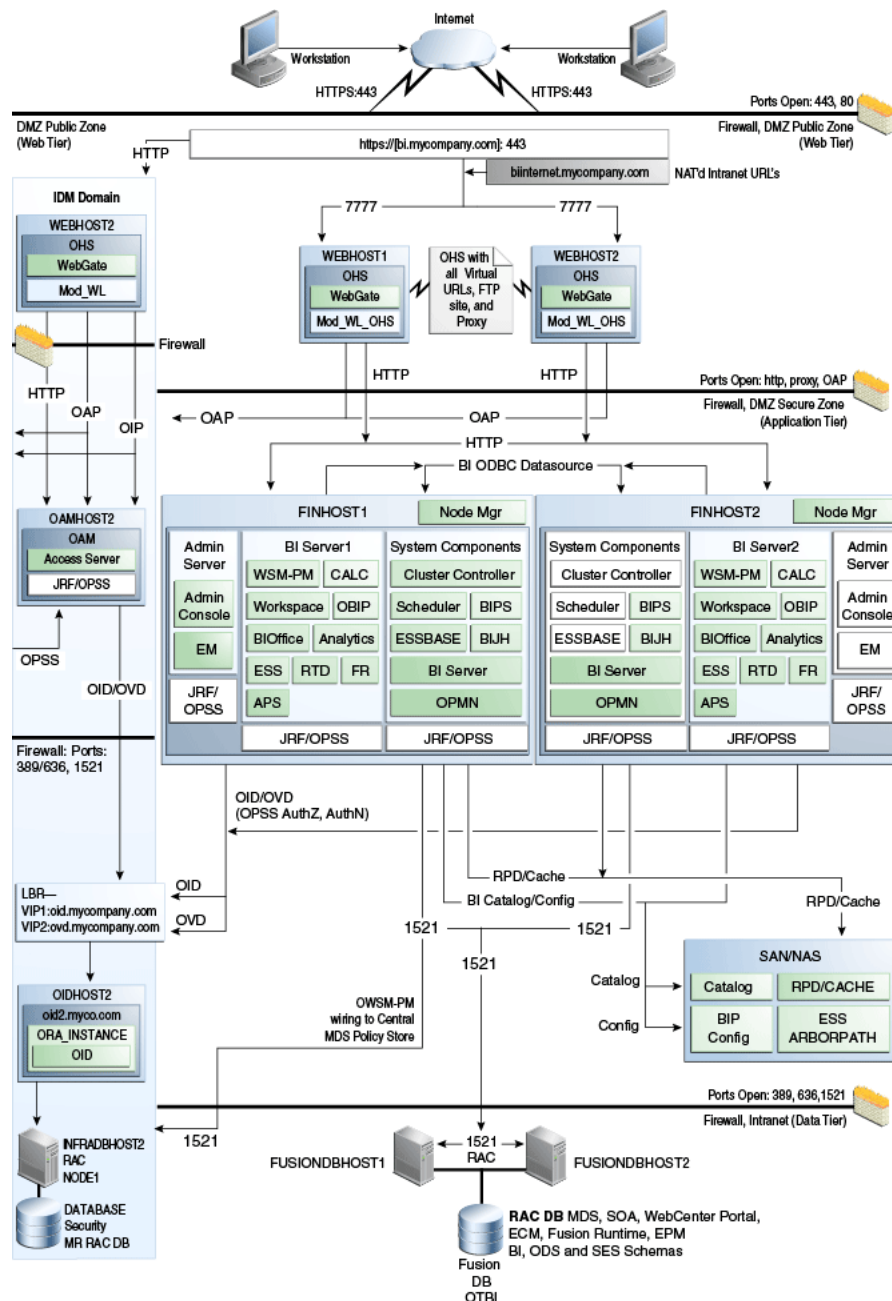
2.1.2.7 Oracle Fusion Procurement Domain

Figure 2–9 shows the Oracle Fusion Procurement domain within the overall reference enterprise deployment topology for Oracle Fusion Applications.

Figure 2–9 Reference Topology for Oracle Fusion Procurement Domain

2.1.2.8 Oracle Business Intelligence Domain

Figure 2–10 shows the Oracle Business Intelligence domain within the overall reference enterprise deployment topology for Oracle Fusion Applications.

Figure 2–10 Reference Topology for Oracle Business Intelligence Domain

2.1.3 About the Web Tier Nodes

Nodes in the Oracle Web Tier are located in the demilitarized zone (DMZ) public zone. In this tier, two nodes *WEBHOST1* and *WEBHOST2* run Oracle HTTP Server configured with WebGate and *FusionVirtualHost_domain.conf*.

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

WebGate (which is an Oracle Access Manager component) in Oracle HTTP Server uses Oracle Access Protocol (OAP) to communicate with Oracle Access Manager running

on *OAMHOST1* and *OAMHOST2*, in the Identity Management DMZ. WebGate and Oracle Access Manager are used to perform operations such as user authentication.

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

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

On the firewall protecting the Oracle Web Tier, only the HTTP ports are open: 443 for HTTPS and 80 for HTTP.

2.1.3.1 Load Balancer Requirements

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

- Ability to load-balance traffic to a pool of real servers through a virtual host name: Clients access services using the virtual host name (instead of using actual host names). The load balancer can then load-balance requests to the servers in the pool.
- Port translation configuration should be possible so that incoming requests on the virtual host name and port are directed to a different port on the back-end servers.
- Monitoring of ports on the servers in the pool to determine availability of a service.
- Virtual servers and port configuration: Ability to configure virtual server names and ports on your external load balancer, and the virtual server names and ports must meet the following requirements:
 - The load balancer should allow configuration of multiple virtual servers. For each virtual server, the load balancer should allow configuration of traffic management on more than one port. For example, for Oracle HTTP Server in the Oracle Web Tier, the load balancer needs to be configured with a virtual server and ports for HTTP and HTTPS traffic.
 - The virtual server names must be associated with IP addresses and be part of your DNS. Clients must be able to access the external load balancer through the virtual server names.
- Ability to detect node failures and immediately stop routing traffic to the failed node.
- Fault-tolerant mode: It is highly recommended that you configure the load balancer to be in fault-tolerant mode.
- It is highly recommended that you configure the load balancer virtual server to return immediately to the calling client when the back-end services to which it forwards traffic are unavailable. This is preferred over the client disconnecting on its own after a timeout based on the TCP/IP settings on the client computer.
- Sticky routing capability: Ability to maintain sticky connections to components. Examples of this include cookie-based persistence, IP-based persistence, and so on.
- The load balancer should be able to terminate SSL requests at the load balancer and forward traffic to the back-end real servers using the equivalent non-SSL protocol (for example, HTTPS to HTTP). Typically, this feature is called SSL acceleration and it is required for this enterprise deployment.

2.1.4 About the Application Tier

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

FINHOST1 and *FINHOST2* run all the Managed Servers in the Oracle Fusion Financials, Oracle Fusion Customer Relationship Management, Oracle Business Intelligence, Oracle Fusion Projects, Oracle Fusion Procurement, Oracle Fusion Supply Chain Management, and Oracle Fusion Human Capital Management domains.

FINHOST1 and *FINHOST2* run the managed and C/C++ servers from different domains in an active-active or active-passive implementation. C/C++ components are managed by Oracle Process Manager and Notification Server (OPMN), and all the Managed Servers are managed by Administration Server within the domain.

FINHOST1 and *FINHOST2* also run the Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control, but in an active-passive configuration. You also can fail over the Administration Server manually. Alternatively, you can configure the Oracle WebLogic Server Administration Console with CFC/CRS to fail over automatically on a separate hardware cluster.

Oracle Web Services Manager (Oracle WSM) provides a policy framework to manage and secure Web services in the enterprise deployment topology. WSM Policy Manager also runs in active-active configuration in every Fusion domain where Web Services are hosted.

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

2.1.5 About the Data Tier

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

In this tier, an Oracle RAC database runs on the nodes *FUSIONDBHOST1* and *FUSIONDBHOST2*. The database contains the schemas needed by the Oracle Fusion Applications components. The components running in the application tier access this database.

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

2.2 Hardware Requirements

This section provides recommended hardware for the Oracle Fusion Applications reference enterprise deployment topology on Linux operating systems.

The recommended hardware for the Oracle Fusion Applications reference enterprise deployment topology consists of six 96 GB Intel Westmere, six dual-core CPU servers (excluding Oracle HTTP Server and Oracle Database servers). [Table 2-1](#) describes the typical hardware requirements.

Table 2–1 Example Hardware Requirements - 200 Concurrent Users

Server	Processor	Memory	TMP	SWAP
<i>FINHOST1</i>	6 core 2 CPU Westmere	96 GB	default	default
<i>FINHOST2</i>	6 core 2 CPU Westmere	96 GB	default	default
<i>FINHOST3</i>	6 core 2 CPU Westmere	96 GB	default	default
<i>WEBHOST1</i>	2 core 2 CPU	4 GB	default	default
<i>WEBHOST2</i>	2 core 2 CPU	4 GB	default	default
<i>FUSIONDBHOST1</i>	4 core 4 CPU	48 GB	default	default
<i>FUSIONDBHOST2</i>	4 core 4 CPU	48 GB	default	default

2.3 Installation Prerequisite

The Oracle Identity Management stack for Oracle Fusion Applications should already be installed prior to starting a deployment. Note, however, that the provisioning process described in [Chapter 5, "Using the Provisioning Process to Install Components for an Enterprise Deployment,"](#) cannot proceed without it. Follow the instructions in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition)* to install and configure these components.

2.4 Implementing the Topology

Oracle recommends the following approach when implementing the Oracle Fusion Applications topology outlined in [Section 2.1, "Overview of Reference Enterprise Deployment Topologies"](#):

1. [Preparing the Network for an Enterprise Deployment](#)
2. [Preparing the Database for an Enterprise Deployment](#)
3. [Using the Provisioning Process to Install Components for an Enterprise Deployment](#)
4. [Scaling Out Oracle HTTP Server](#)
5. [Setting Up Node Manager for an Enterprise Deployment](#)
6. [Scaling Out the Oracle Fusion Financials Domain](#)
7. [Scaling Out the Oracle Fusion Customer Relationship Management Domain](#)
8. [Scaling Out the Oracle Fusion Common Domain](#)
9. [Scaling Out the Oracle Fusion Human Capital Management Domain](#)
10. [Scaling Out the Oracle Fusion Supply Chain Management Domain](#)
11. [Scaling Out the Oracle Fusion Projects Domain](#)
12. [Scaling Out the Oracle Fusion Procurement Domain](#)
13. [Scaling Out the Oracle Business Intelligence Domain](#)
14. [Additional Configuration Procedures for Scaling Out Oracle SOA Suite Server](#)
15. [Configuring Administration Server High Availability](#)
16. [Setting Up Server Migration for an Enterprise Deployment](#)
17. [Configuring Oracle Business Intelligence Applications](#)

18. [Managing the Topology](#)**19. [Deploying Administrative Clients for Oracle Fusion Applications](#)**

Oracle recommends this modular approach in order to facilitate the verification of individual components one by one. This building block approach simplifies the troubleshooting during the setup process and facilitates the configuration in smaller steps.

Preparing the Network for an Enterprise Deployment

This chapter describes the network environment configuration required by the Oracle Fusion Applications reference enterprise deployment topology, as well as recommendations for shared storage and directory structure.

This chapter includes the following topics:

- [Section 3.1, "External Virtual Server Names"](#)
- [Section 3.2, "Internal Virtual IPs"](#)
- [Section 3.3, "Load Balancer Configuration"](#)
- [Section 3.4, "Reference Enterprise Deployment Directory Structure"](#)
- [Section 3.5, "Shared Storage"](#)
- [Section 3.6, "IPs and Virtual IPs"](#)
- [Section 3.7, "Firewalls and Ports"](#)
- [Section 3.8, "Clock Synchronization"](#)

3.1 External Virtual Server Names

The Oracle Fusion Applications enterprise deployment topology uses the following externally accessible load balancer virtual IPs that are created on the Load Balancer:

- *finexternal.mycompany.com*
- *prjexternal.mycompany.com*
- *prcexternal.mycompany.com*
- *prcsupplierportal-external.mycompany.com*
- *crmexternal.mycompany.com*
- *hcmexternal.mycompany.com*
- *scmexternal.mycompany.com*
- *biexternal.mycompany.com*
- *commonexternal.mycompany.com*

These virtual server names act as the access point for all HTTP traffic to the runtime components for Oracle Fusion Financials. The HTTP traffic from client browser to LBR is always in SSL.

These VIPs receive all the requests externally (from the intranet or internet) on port 443 in SSL mode. These requests are forwarded to one of Oracle HTTP Server's "external virtual hosts specific to each domain" on *WEBHOST1* or *WEBHOST2*.

Note: All external VIPs listed above are also configured on port 80, and any request that is received on port 80 will be forwarded back to port 443. This is to prevent a browser error when the user types the URL without the `http://` and the browser uses the default 80 port. If the user types `https://`, the browser uses the default 443 port.

3.2 Internal Virtual IPs

The following Oracle Fusion Financials deployment topology also requires separate secure network address translations (NATs) internal VIPs for each domain. These VIPs are used for transactional and administrative access.

- *fininternal.mycompany.com*
- *prjinternal.mycompany.com*
- *prcinternal.mycompany.com*
- *prcsupplierportal-internal.mycompany.com*
- *crminternal.mycompany.com*
- *hcminternal.mycompany.com*
- *scminternal.mycompany.com*
- *biinternal.mycompany.com*
- *commoninternal.mycompany.com*

The above virtual URLs (VIPs) are defined on the load balancer and are used for internal invocations of services within the data center. The URLs are not exposed to the internet or intranet, and are only accessible within the data center.

The VIPs receive all the requests internally on port 7777 in non-SSL mode. All the internal services/clients access these VIPs using the above virtual addresses, and the requests are then forwarded to one of Oracle HTTP Server's "internal virtual hosts specific to each domain" on *WEBHOST1* or *WEBHOST2*.

For additional Oracle WebLogic Server security, you can configure the internal VIPs listed above with a load-balancing router rule that accepts requests only from well-known hosts like *FINHOST1*, *FINHOST2*, or from the system administrator host, and rejects all other requests.

3.3 Load Balancer Configuration

The Oracle Fusion Applications enterprise topology requires an external load balancer with SSL acceleration. To configure the load balancer with above VIPs listed above, refer to vendor-specific load balancer configuration instructions.

Note: The Oracle Technology Network (<http://otn.oracle.com>) provides a list of validated load balancers and their configurations.

3.4 Reference Enterprise Deployment Directory Structure

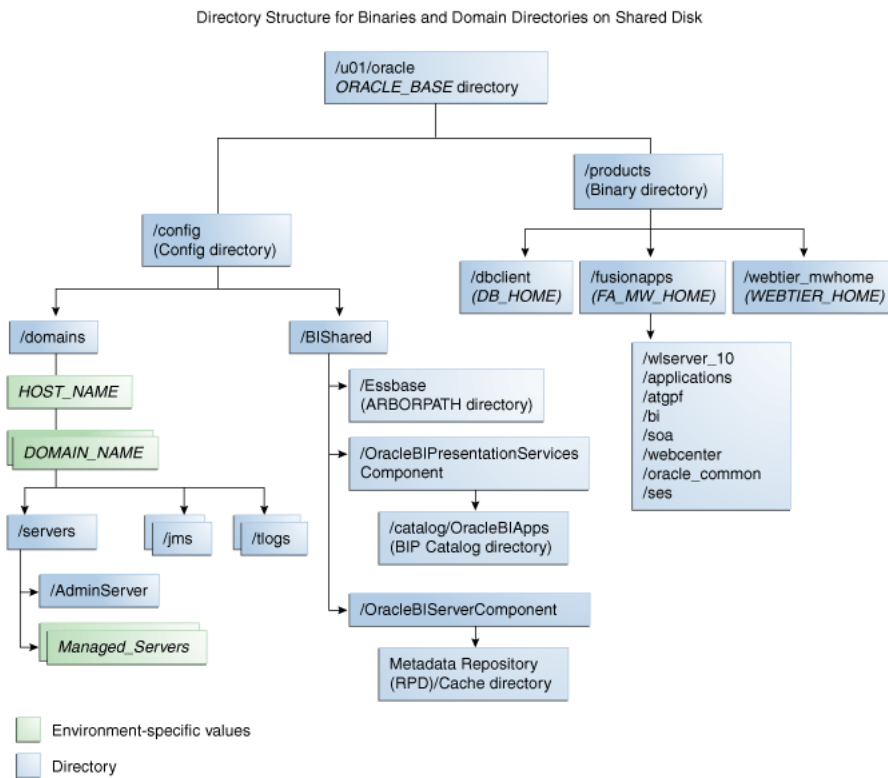
This section describes the directory structure specifically used by the Oracle Fusion Applications reference enterprise deployment topology. It includes the following topics:

- [Section 3.4.1, "Directory Structure"](#)
- [Section 3.4.2, "Binary Directory Structure"](#)
- [Section 3.4.3, "Domain Configuration Directory Structure"](#)

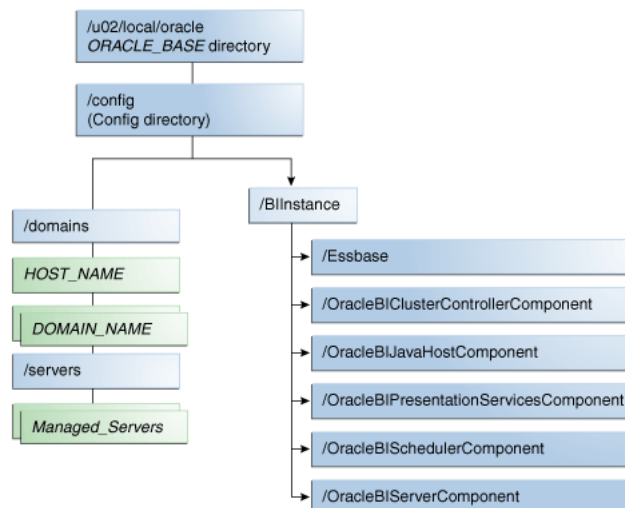
For general information about Oracle Fusion Applications architecture and concepts, see "Introduction to Oracle Fusion Applications for System Administrators" in *Oracle Fusion Applications Administrator's Guide*.

3.4.1 Directory Structure

[Figure 3–1](#) shows the enterprise deployment directory structure and its dependencies.

Figure 3–1 Enterprise Deployment Directory Structure for Oracle Fusion Applications

Directory Structure for Binaries and Domain Directories on Local Disk



3.4.2 Binary Directory Structure

The binaries in the Oracle Fusion Applications reference enterprise deployment topology (the Oracle Fusion Middleware home and Oracle home) are on a shared disk. In order to avoid disk corruption, you may choose to maintain snapshots.

The file system for the binaries should be mounted on all the nodes with the exact mount point and path. For example, /u01/oracle.

3.4.3 Domain Configuration Directory Structure

The domain configuration directory structure is created on a shared disk, and its mount point should be visible from all nodes. This path will be used by the components that require shared resources and also administration servers to start active-passive processes. For example, `/u01/oracle`.

3.5 Shared Storage

For binaries: the file system is optimized for read operations.

For config: the file system should be optimized for read/write operations. For example, AdminServer Domain directory and Oracle Business Intelligence shared folders like Oracle Business Intelligence WebCat, RPD cache, Essbase ARBORPATH, and Oracle Business Intelligence config.

Note: The minimum amount of shared storage is 500 GB.

The following steps show how to create and mount shared storage locations for binaries and config so that *FINHOST1* and *FINHOST2* can see the same location.

"nasfiler" is the shared storage filer.

From *FINHOST1*:

```
FINHOST1> mount nasfiler:/vol/vol1/u01/oracle /u01/oracle -t nfs
```

From *FINHOST2*:

```
FINHOST2> mount nasfiler:/vol/vol1/u01/oracle /u01/oracle -t nfs
```

Note: The shared storage can be a NAS or SAN device. The following illustrates an example of creating storage for a NAS device from *FINHOST1*. The options may differ.

```
mount nasfiler:/vol/vol1/u01/oracle
/u01/oracle -t nfs -o
rw,bg,hard,nointr,tcp,vers=3,timeo=300,rsize=32768,
wsize=32768
```

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

3.5.1 Shared Storage for Oracle Business Intelligence

For general information, see "Shared Storage and Recommended Directory Structure" in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence*.

Shared Storage Locations

In addition, Oracle Business Intelligence has two specific shared-storage locations.

- Location for Data Warehouse Console Configuration folder:

```
ORACLE_BASE/config/BIShared/dac
```

- Mounted from: All nodes containing the instance of DAC in the cluster or where DAC can be migrated to must mount this location (all nodes must have read/write access)
- Location for shared Essbase ARBORPATH:
`ORACLE_BASE/config/BIShared/Essbase`
 - Mounted from: All nodes containing the instance of Essbase in the cluster must mount this location (all nodes must have read/write access)

Note: `ORACLE_BASE` is `/u01/oracle`.

3.6 IPs and Virtual IPs

Configure the Administration Server and the Managed Servers to listen on different virtual IPs and physical IPs.

The following VIPs are required to configure specific components:

- Virtual IPs for AdminServer are needed for every domain to configure AdminServer in active-passive mode. These VIPs are shared across `FINHOST1` and `FINHOST2`, depending on where the Administration Server is running.
- Virtual IPs for all Oracle SOA Suite servers in every domain, and Oracle Business Intelligence servers in the Oracle Business Intelligence domain are needed to support server migration. These components are implemented in active-active mode, so these VIPs are needed for `FINHOST1` and `FINHOST2`.

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

Table 3–1 Virtual Hosts

Virtual IP	VIP Maps to...	Description
VIP1	<code>FINADMINVH</code>	The virtual host name that is the listen address for the FinancialDomain Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the FinancialDomain Administration Server process is running (<code>FINHOST1</code> by default).
VIP2	<code>FINSOAVH1</code>	The virtual host name that maps to the listen address for <code>soa_server1</code> and fails over with server migration of this Managed Server. It is enabled on the node where <code>soa_server1</code> process is running (<code>FINHOST1</code> by default).
VIP3	<code>FINSOAVH2</code>	The virtual host name that maps to the listen address for <code>soa_server2</code> and fails over with server migration of this Managed Server. It is enabled on the node where <code>soa_server2</code> process is running (<code>FINHOST2</code> by default).
VIP4	<code>COMMONADMINVH</code>	The virtual host name that is the listen address for the CommonDomain Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the CommonDomain Administration Server process is running (<code>FINHOST1</code> by default).
VIP5	<code>COMMONSOAVH1</code>	The virtual host name that maps to the listen address for <code>soa_server1</code> and fails over with server migration of this Managed Server. It is enabled on the node where <code>soa_server1</code> process is running (<code>FINHOST1</code> by default).

Table 3–1 (Cont.) Virtual Hosts

Virtual IP	VIP Maps to...	Description
VIP6	<i>COMMONSOAVH2</i>	The virtual host name that maps to the listen address for <i>soa_server2</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>soa_server2</i> process is running (<i>FINHOST2</i> by default).
VIP7	<i>COMMONIPMVH1</i>	The virtual host name that maps to the listen address for <i>IPM_server1</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>IPM_server1</i> process is running (<i>FINHOST1</i> by default).
VIP8	<i>COMMONIPMVH2</i>	The virtual host name that maps to the listen address for <i>IPM_server2</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>IPM_server2</i> process is running (<i>FINHOST2</i> by default).
VIP9	<i>CRMADMINVH</i>	The virtual host name that is the listen address for the CRMDomain Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the CRMDomain Administration Server process is running (<i>FINHOST1</i> by default).
VIP10	<i>CRMSOAVH1</i>	The virtual host name that maps to the listen address for <i>soa_server1</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>soa_server1</i> process is running (<i>FINHOST1</i> by default).
VIP11	<i>CRMSOAVH2</i>	The virtual host name that maps to the listen address for <i>soa_server2</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>soa_server2</i> process is running (<i>FINHOST2</i> by default).
VIP12	<i>HCMADMINVH</i>	The virtual host name that is the listen address for the HCMDomain Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the HCMDomain Administration Server process is running (<i>FINHOST1</i> by default).
VIP13	<i>HCMSOAVH1</i>	The virtual host name that maps to the listen address for <i>soa_server1</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>soa_server1</i> process is running (<i>FINHOST1</i> by default).
VIP14	<i>HCMSOAVH2</i>	The virtual host name that maps to the listen address for <i>soa_server2</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>soa_server2</i> process is running (<i>FINHOST2</i> by default).
VIP15	<i>SCMADMINVH</i>	The virtual host name that is the listen address for the SCMDomain Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the SCMDomain Administration Server process is running (<i>FINHOST1</i> by default).
VIP16	<i>SCMSOAVH1</i>	The virtual host name that maps to the listen address for <i>soa_server1</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>soa_server1</i> process is running (<i>FINHOST1</i> by default).
VIP17	<i>SCMSOAVH2</i>	The virtual host name that maps to the listen address for <i>soa_server2</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>soa_server2</i> process is running (<i>FINHOST2</i> by default).

Table 3–1 (Cont.) Virtual Hosts

Virtual IP	VIP Maps to...	Description
VIP18	<i>BIADMINVH</i>	The virtual host name that is the listen address for the BIDomain Administration Server. It is enabled on the node where the BIDomain Administration Server process is running (<i>FINHOST1</i> by default).
VIP19	<i>BIVH1</i>	The virtual host name that maps to the listen address for <i>bi_server1</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>bi_server1</i> process is running (<i>FINHOST1</i> by default).
VIP20	<i>BIVH2</i>	The virtual host name that maps to the listen address for <i>bi_server2</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>bi_server2</i> process is running (<i>FINHOST2</i> by default).
VIP21	<i>PRJSOAVH1</i>	The virtual host name that maps to the listen address for <i>soa_server1</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>soa_server1</i> process is running (<i>FINHOST1</i> by default).
VIP22	<i>PRJADMINVH</i>	The virtual host name that is the listen address for the ProjectsDomain Administration Server. It is enabled on the node where the ProjectsDomain Administration Server process is running (<i>FINHOST1</i> by default).
VIP23	<i>PRJSOAVH2</i>	The virtual host name that maps to the listen address for <i>soa_server2</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>soa_server2</i> process is running (<i>FINHOST2</i> by default).
VIP24	<i>PRCSOAVH1</i>	The virtual host name that maps to the listen address for <i>soa_server1</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>soa_server1</i> process is running (<i>FINHOST1</i> by default).
VIP 25	<i>PRCADMINVH</i>	The virtual host name that is the listen address for the ProcurementDomain Administration Server and fails over with manual failover of the Administration Server. It is enabled on the node where the ProcurementDomain Administration Server process is running (<i>FINHOST1</i> by default).
VIP 26	<i>PRCSOAVH2</i>	The virtual host name that maps to the listen address for <i>soa_server2</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>soa_server2</i> process is running (<i>FINHOST2</i> by default).
VIP27	<i>FINSOAVH3</i>	The virtual host name that maps to the listen address for <i>soa_server3</i> and fails over with server migration of this Managed Server. It is enabled on the node where <i>soa_server3</i> process is running (<i>FINHOST3</i> by default).
VIP28	<i>FUSIONDBHOST1</i>	The virtual host name that is the listen address for the database Oracle RAC database server. It is enabled on the node where the database is running.

3.7 Firewalls and Ports

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

Most port numbers are assigned during installation.

Table 3–2 lists the ports used in the Oracle Fusion Financials topology, including 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 Oracle Web Tier and the application tier
- FW3 refers to the firewall between the application tier and the data tier
- dst refers to destination

Table 3–2 Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Browser request	FW1	80 (dst)	HTTP	Inbound	Timeout depends on all HTML content and the type of process model used for Oracle Fusion Applications.
Browser request	FW1	443	HTTPS / Load Balancer	Inbound	Timeout depends on all HTML content and the type of process model used for Oracle Fusion Applications.
Browser request	FW1	443 (dst)	HTTPS	Outbound	Open connection to http://xmlns.oracle.com/adf/config only
OAP	N/A	8181	HTTP	N/A	
Oracle HTTP Server registration with Administration Server	FW2	7001 (both)	HTTP/t3	Inbound	Set the timeout to a short period (5-10 seconds).
Oracle HTTP Server registration with Administration Server	FW2	OPMN port 7043 (dst) and Oracle HTTP Server Admin Port 7044 (dst)	TCP and HTTP, respectively	Outbound	Set the timeout to a short period (5-10 seconds).
All Domain Servers	FW2	7777 (dst)	HTTP	Outbound	Managed Servers are sending packets to LBR internal VIPs with port 7777
All Domains: Server Migration and Multicast VIPs	FW2		Multicast	Outbound	
Common Domain	FW2	7001-7035 (dst)	HTTP	Inbound	
Financial Domain	FW2	7401-7430 (dst)	HTTP	Inbound	
Supply Chain Domain	FW2	7801-7830 (dst)	HTTP	Inbound	
Customer Relationship Management Domain	FW2	9001-9040 (dst)	HTTP	Inbound	
Human Capital Management Domain	FW2	9401-9430 (dst)	HTTP	Inbound	

Table 3–2 (Cont.) Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Business Intelligence Domain	FW2	10201-10230 (dst)	HTTP	Inbound	
Common Administration Console access	FW2	7001 (both)	HTTP / Administration Server and Enterprise Manager t3	Both	You should tune this timeout based on the type of access to the administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
Financial Administration Console access	FW2	7401 (both)	HTTP / Administration Server and Enterprise Manager t3	Both	You should tune this timeout based on the type of access to the administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
Projects Domain	FW2	8601-9000 (dst)	HTTP	Inbound	
Procurement Domain	FW2	8201-8600 (dst)	HTTP	Inbound	
SCM Administration Console access	FW2	7801 (both)	HTTP / Administration Server and Enterprise Manager t3	Both	You should tune this timeout based on the type of access to the administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
FIN Administration Console access	FW2	9001 (both)	HTTP / Administration Server and Enterprise Manager t3	Both	You should tune this timeout based on the type of access to the administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).

Table 3–2 (Cont.) Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
HCM Administration Console access	FW2	9401 (both)	HTTP / Administration Server and Enterprise Manager t3	Both	You should tune this timeout based on the type of access to the administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
BI Administration Console access	FW2	10201 (both)	HTTP / Administration Server and Enterprise Manager t3	Both	You should tune this timeout based on the type of access to the administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
PRJ Administration Console access	FW2	8601	HTTP / Administration Server and Enterprise Manager t3	Both	You should tune this timeout based on the type of access to the administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
PRC Administration Console access	FW2	8201	HTTP / Administration Server and Enterprise Manager t3	Both	You should tune this timeout based on the type of access to the administration console (whether it is planned to use the Oracle WebLogic Server Administration Console from application tier clients or clients external to the application tier).
Node Manager	N/A	5556	TCP/IP	N/A	N/A
Access Server access	FW2	5574-5575	OAP	Both	For actual values, see "Firewalls and Ports" in <i>Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management</i> .
Identity Server access	FW2	6022	OAP	Inbound	

Table 3–2 (Cont.) Ports Used

Type	Firewall	Port and Port Range	Protocol / Application	Inbound / Outbound	Other Considerations and Timeout Guidelines
Database access for Oracle BI Server and Oracle BI Publisher JDBC Data Sources	FW2	Listening port for client connections to the listener (both)	SQL*Net	Both	Timeout depends on all database content and on the type of process model used for Oracle BI
Database access	FW3	1521 (both)	SQL*Net	Both	Timeout depends on all database content and on the type of process model used for Oracle Fusion Applications.
Coherence for deployment	N/A	8088 and 8089 (both)		N/A	N/A
Oracle Internet Directory access	FW3	389 (dst)	LDAP	Inbound	You should tune the directory server's parameters based on load balancer, and not the other way around.
Oracle Internet Directory access	FW3	636 (dst)	LDAP SSL	Inbound	You should tune the directory server's parameters based on load balancer, and not the other way around.
JOC for OWSM	N/A	9991	TCP/IP	N/A	N/A

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

3.8 Clock Synchronization

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

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

Preparing the Database for an Enterprise Deployment

This chapter provides information about how the database tier is implemented in an enterprise deployment topology.

This chapter includes the following topics:

- [Section 4.1, "Understanding the Database in the Enterprise Deployment Topology"](#)
- [Section 4.2, "Setting Up the Database"](#)
- [Section 4.3, "Creating and Starting the Database Services"](#)
- [Section 4.4, "Loading the Oracle Fusion Applications Repository into the Oracle RAC Database"](#)
- [Section 4.5, "Backing Up the Database"](#)

4.1 Understanding the Database in the Enterprise Deployment Topology

The Oracle Fusion Applications reference enterprise deployment topology uses a single database for the following components:

- Oracle Fusion Applications metadata
- Oracle Fusion Applications transactional data
- Oracle Transactional Business Intelligence data
- Technology stack data, such as Oracle SOA Suite, Oracle Enterprise Manager Fusion Middleware Control, Oracle WebCenter Portal, and Oracle Essbase.
- Oracle Secure Enterprise Search data

Implementing Oracle Business Intelligence Data Warehouse requires a separate database for following components:

- Data Warehouse Administration Console (DAC)
- Informatica
- a Data Warehouse

For the enterprise topology, Oracle Real Application Clusters (Oracle RAC) databases are highly recommended. You must set up these databases before you can install and configure the Oracle Fusion Applications components. You install the Oracle Fusion Applications and Oracle Fusion Middleware metadata repositories into existing databases using the Fusion Applications Repository Creation Utility (Fusion Applications RCU).

4.2 Setting Up the Database

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

- [Database Host Requirements](#)
- [Supported Database Versions](#)
- [Minimum Database Configuration Parameters](#)

Note: When creating the database, ensure that the length of the Oracle System ID (SID) does not exceed eight (8) characters.

For example:

- *SID: abcd12345* is invalid
 - *SID: abcd123* is valid
-
-

4.2.1 Database Host Requirements

Note the following requirements for the hosts *FUSIONDBHOST1* and *FUSIONDBHOST2* in the data tier:

- **Oracle Clusterware**
For Oracle Database 11g Release 2 (11.2.0.2) for Linux, refer to the *Oracle Database Installation Guide*.
- **Oracle Real Application Clusters**
For Oracle RAC 11g Release 2 (11.2.0.2) for Linux or Oracle Database 10g Release 2 (10.2) for Linux, refer to the *Oracle Database Installation Guide*.
- **Oracle Automatic Storage Management (optional)**
Oracle ASM gets installed for the node as a whole. It is recommended that you install it in a separate Oracle Home from the Database Oracle Home. This option comes in at runInstaller. In the Select Configuration page, select the **Configure Automatic Storage Management** option to create a separate Oracle ASM home.

4.2.2 Supported Database Versions

Oracle Fusion Applications requires the presence of a supported database and schemas. To check if your database is certified or to see all certified databases, refer to the supported platforms documentation for Oracle Fusion Applications.

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

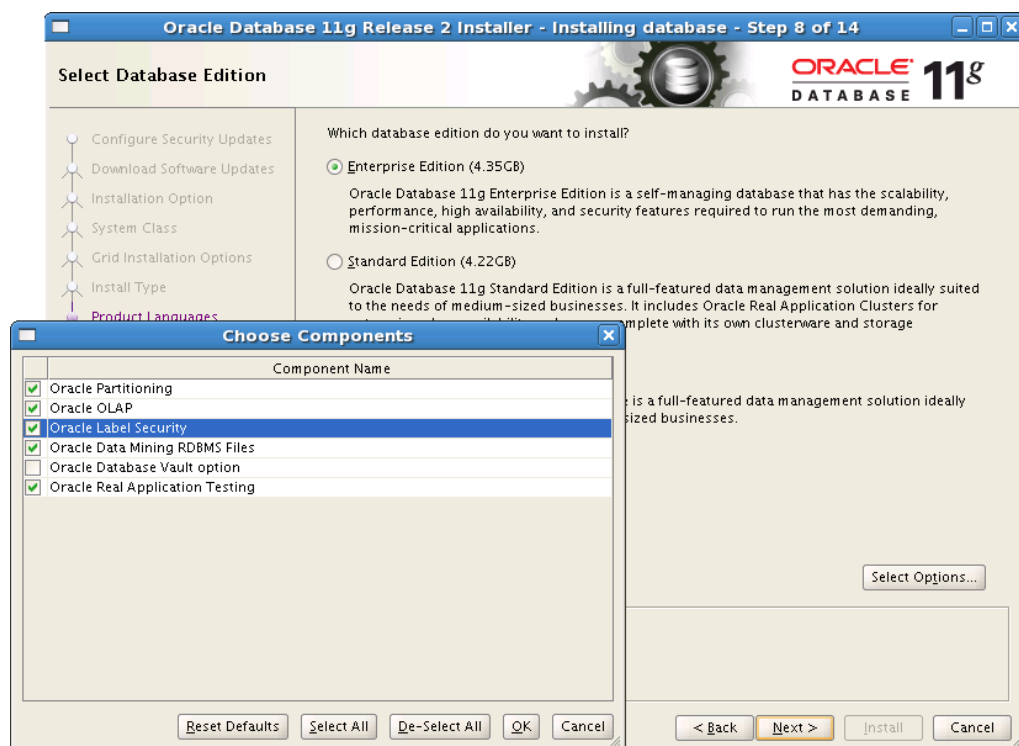
```
SQL> SELECT VERSION FROM SYS.PRODUCT_COMPONENT_VERSION WHERE PRODUCT LIKE  
'Oracle%';
```

Notes:

- The database you use as the Oracle Fusion Applications supporting database must support the AL32UTF8 character set.
- When installing the database, please ensure that **Oracle Label Security** is enabled, as shown in [Figure 4-1](#). In the case of an Oracle RAC installation, the Oracle Label Security should be enabled on all the nodes.

You enable label security in the Select Database Edition screen, shown in [Figure 4-1](#), using Oracle Universal Installer.

Figure 4-1 Oracle Label Security



4.2.3 Minimum Database Configuration Parameters

[Table 4-1](#) shows the recommended minimum init.ora parameters for an Oracle database. The database shipped with the Oracle Fusion Applications software contains this configuration. When you run the Fusion Applications RCU, its prerequisite check feature checks to see that the database meets these minimum requirements.

Table 4-1 Minimum Requirements for Database Configuration

INST_ID Parameter	Value
_b_tree_bitmap_plans	FALSE
audit_trail	NONE
compatible	11.2.0
db_files	1024

Table 4–1 (Cont.) Minimum Requirements for Database Configuration

INST_ID Parameter	Value
db_recovery_file_dest_size	2147483648
db_writer_processes	1
disk_asynch_io	FALSE
fast_start_mttr_target	3600
filesystemio_options	Setall
job_queue_processes	10
log_buffer	10485760
log_checkpoints_to_alert	TRUE
max_dump_file_size	10M
memory_target	unset or N/A
nls_sort	BINARY
open_cursors	500
pga_aggregate_target	>= 4294967296 (4GB)
plsql_code_type	NATIVE
processes	5000
session_cached_cursors	500
sga_target	>=9663676416 (9GB)
trace_enabled	FALSE
undo_management	AUTO

For example, to use the `SHOW PARAMETER` command using SQL*Plus to check the value of the initialization parameter:

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

```
SQL> SHOW PARAMETER processes
```

2. Set the initialization parameter using the following commands:

```
SQL> ALTER SYSTEM SET processes=5000 SCOPE=SPFILE;
```

```
SQL> ALTER SYSTEM SET open_cursors=500 SCOPE=SPFILE;
```

3. Restart the database.

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

4.3 Creating and Starting the Database Services

Oracle recommends using the Oracle Enterprise Manager Fusion Middleware Control Cluster Managed Services screen or SQL*Plus to create database services that client applications will use to connect to the database.

To configure this using SQL*Plus:

1. Use the `CREATE_SERVICE` subprogram to create the database service.

Log in to SQL*Plus as the `sysdba` user and run the following command:

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

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

```
prompt> srvctl add service -d fusiondb -s fin.mycompany.com -r
fusiondb1,fusiondb2
```

3. Start the service using `srvctl`:

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

4. Verify that the `fin` service is running on instance(s) `fusiondb1` and `fusiondb2`:

```
prompt> srvctl status service -d fusiondb
```

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

Oracle recommends that a specific database service be used for a product suite even when they share the same database. It is also recommended that the database service used is different than the default database service. For example, for Oracle Fusion Financials the database would be `findb.mycompany.com` and the default service is one with the same name. The Oracle Fusion Financials install is configured to use the service `fin.mycompany.com`.

4.3.1 Updating the Kernel Parameters

This section describes how to update the kernel parameters for Linux before the database is installed.

To update the parameters:

1. Log in as root and add or edit the following values in the `/etc/sysctl.conf` file:

```
fs.file-max = 6815744
kernel.shmall = 2097152
kernel.shmmax = 2147483648
kernel.shmmni = 4096
kernel.sem = 250 32000 100 128
net.core.rmem_default = 4194304
net.core.rmem_max = 4194304
net.core.wmem_default = 262144
net.core.wmem_max = 1048576
net.ipv4.ip_forward = 0
net.ipv4.conf.default.rp_filter = 1
tcp.ipv4.tcp_wmem = 262144 262144 262144
```

```
tcp.ipv4.tcp_rmem = 4194304 4194304 4194304
fs.aio-max-nr = 1048576
net.ipv4.ip_local_port_range = 9000 65000
```

2. Execute the following command to activate the changes:

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

4.4 Loading the Oracle Fusion Applications Repository into the Oracle RAC Database

Before loading the Oracle Fusion Applications repository into a database, you must apply database patch 10220058 in order to run the Oracle Fusion Applications Repository Creation Utility (Fusion Applications RCU) with Oracle Database 11g Enterprise Edition Release 11.2.0.2.0. To find the patch, go to My Oracle Support (<https://support.oracle.com>) and click the **Patches & Updates** tab.

The Fusion Applications RCU components are included in the zipped Fusion Applications RCU file delivered in the provisioning framework. (The location of the file is `ORACLE_BASE/installers/apps_rcu/linux/rcuHome_fusionapps_linux.zip`.) Unzip the file to the `RCU_HOME` location on the `FUSIONDBHOST1` machine. For example, `ORACLE_BASE/rcu`.

Once you have the Fusion Applications RCU installed, do the following:

1. Copy all the required dump files locally on `FUSIONDBHOST1` (for example, to `/tmp`):

```
FUSIONDBHOST1> cd RCU_HOME/rcu/integration/fusionapps
FUSIONDBHOST1> cp export_fusionapps_dbinstall.zip /tmp
FUSIONDBHOST1> cd RCU_HOME/rcu/integration/biapps/schema
FUSIONDBHOST1> cp otbi.dmp /tmp
FUSIONDBHOST1> cd /tmp
FUSIONDBHOST1> unzip export_fusionapps_dbinstall.zip
```

Note: When running Fusion Applications RCU for Oracle RAC, you must copy the `export_fusionapps_dbinstall.zip` file as well as `otbi.dmp` to all the nodes of the Oracle RAC.

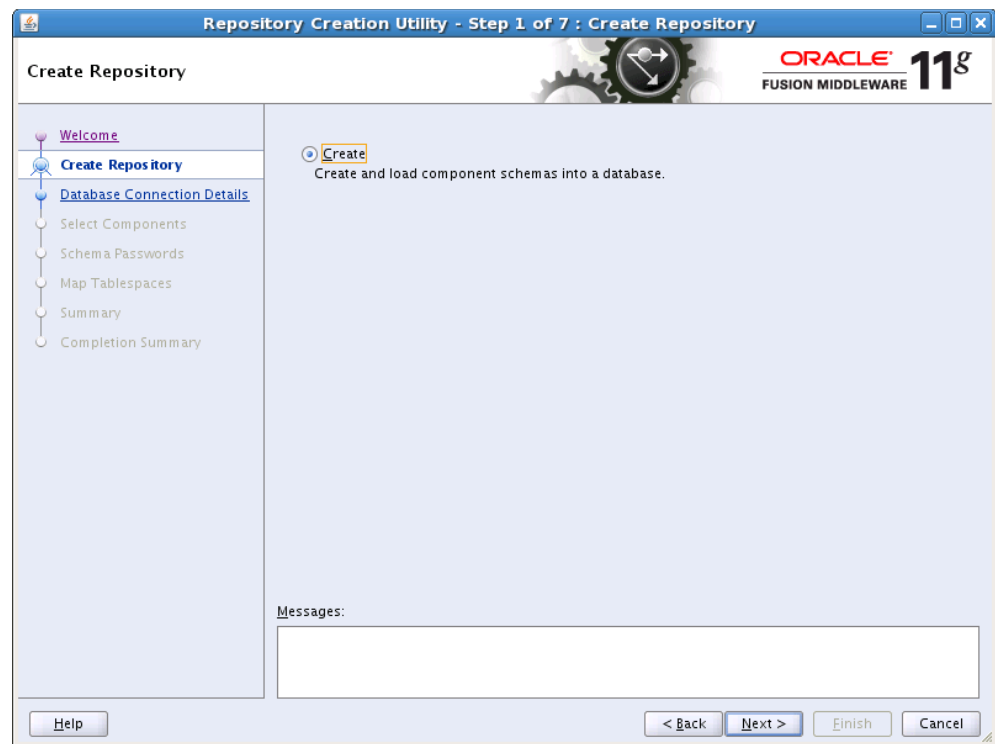
2. Create the `incident_logs` directory on `FUSIONDBHOST1`:

```
FUSIONDBHOST1> cd ORACLE_HOME
FUSIONDBHOST1> mkdir incident_logs
```

3. Start Fusion Applications RCU from the `/bin` directory in the Fusion Applications RCU home directory:

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

4. In the Welcome screen (if displayed), click **Next**.
5. In the Create Repository screen, shown in [Figure 4–2](#), select **Create** to load component schemas into a database. Click **Next**.

Figure 4–2 Create Repository Screen

6. In the Database Connection Details screen, shown in [Figure 4–3](#), enter connect information for your database:
 - **Database Type:** Select **Oracle Database**
 - **Host Name:** Specify the name of the node on which the database resides. For the Oracle RAC database, specify the VIP name or one of the node names as the host name: *FUSIONDBHOST1-VIP*
 - **Port:** Specify the listen port number for the database; for example 1521
 - **Service Name:** Specify the service name of the database (*fin.mycompany.com*)
 - **Username:** Specify the name of the user with DBA or SYSDBA privileges: *SYS*
 - **Password:** Enter the password for the SYS user
 - **Role:** Select the database user's role from the list: *SYSDBA* (required by the SYS user)

Click **Next**.

Figure 4–3 Database Connection Details Screen

Repository Creation Utility - Step 2 of 7 : Database Connection Details

Database Connection Details

Database Type: Oracle Database

Host Name: FUSIONDBHOST1-VIP
For RAC database, specify VIP name or one of the Node name as Host name.

Port: 1521

Service Name: fin.mycompany.com

Username: sys
User with DBA or SYSDBA privileges. Example:sys

Password: ••••••••

Role: SYSDBA
One or more components may require SYSDBA role for the operation to succeed.

Repository Creation Utility - Checking Prerequisites

Checking Global Prerequisites

✓ Initializing repository configuration metadata	00:00.716(ms)
✓ Obtain properties of the specified database	00:00.101(ms)
✓ Check requirement for specified database	00:00.306(ms)
✓ Execute pre create operations	00:00.306(ms)

Operation completed. Click OK to continue to next page.

OK < Back Next > Finish Cancel

7. The Repository Creation Utility selects the required components automatically, as shown in [Figure 4–4](#).

Figure 4–4 Select Components Screen

Repository Creation Utility - Step 3 of 7 : Select Components

Select Components

A Prefix groups the components associated with one deployment.

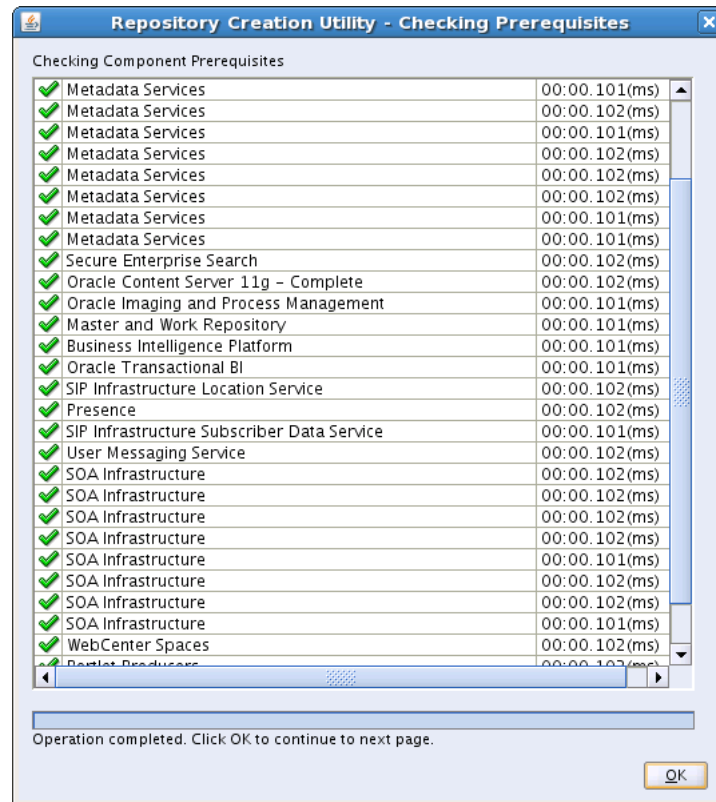
Component	Schema Owner
☐ Oracle AS Repository Components	
☒ Fusion Applications	
☒ Fusion Applications	FUSION
☒ AS Common Schemas	
☒ Enterprise Scheduler Service	FUSION_ORA_ESS
☒ Metadata Services	CRM_FUSION_MDS_SOA
☒ Metadata Services	FIN_FUSION_MDS_SOA
☒ Metadata Services	HCM_FUSION_MDS_SOA
☒ Metadata Services	OIC_FUSION_MDS_SOA
☒ Metadata Services	PRC_FUSION_MDS_SOA
☒ Metadata Services	PRJ_FUSION_MDS_SOA
☒ Metadata Services	SCM_FUSION_MDS_SOA
☒ Metadata Services	SETUP_FUSION_MDS_SOA
☒ Metadata Services	FUSION_MDS
☒ Metadata Services	FUSION_MDS_ESS
☒ Metadata Services	FUSION_MDS_SPACES
☒ Secure Enterprise Search	
☒ Secure Enterprise Search	SEARCHSYS
☒ Enterprise Content Management	
☒ Oracle Content Server 11g - Complete	FUSION_OCSERVER11G

Messages:

Help < Back Next > Finish Cancel

Click **Next**. The Repository Creation Utility checks the prerequisites, as shown in Figure 4-5.

Figure 4-5 Prerequisite Check



Click **OK**.

8. In the Schema Passwords screen, shown in Figure 4-6, enter passwords for the main and additional (auxiliary) schema users, and click **Next**.

Note: For increased security, do the following:

- Specify different schema passwords for all schemas
 - Ensure that all passwords are more than eight (8) characters in length.
-

Figure 4–6 Schema Passwords Screen

Repository Creation Utility - Step 4 of 8 : Schema Passwords

Schema Passwords

Please enter the passwords for the main and additional (auxiliary) schema users. Password can contain alphabets, numbers and the following special characters: \$, #, _ . Password should not start with a number or a special character.

☒ Use same passwords for all schemas

Password:

Confirm Password:

☐ Use main schema passwords for auxiliary schemas

☐ Specify different passwords for all schemas

Component	Schema Owner	Schema Passw...	Confirm Passw...
Fusion Applications	FUSION		
Auxiliary Schema	FUSION_DYNAMIC		
Auxiliary Schema	FUSION_RUNTIME		
Auxiliary Schema	FUSION_APM		
Auxiliary Schema	FUSION_AQ		
Auxiliary Schema	FUSION_BI		
Auxiliary Schema	FUSION_DQ		
Auxiliary Schema	FUSION_ODI_STAGE		
Enterprise Scheduler Service	FUSION_ORA_ESS		
Metadata Services	CRM_FUSION_MDS_SOA		
Metadata Services	FIN_FUSION_MDS_SOA		

Messages:

9. In the Custom Variables screen, shown in [Figure 4–7](#), enter the required values.

Fusion Applications

- **FUSIONAPPS_DBINSTALL_DP_DIR:** The directory on the database server where you unzipped export_fusionapps_dbinstall.zip and copied the otbi.dmp file. For example, /tmp.
- **APPLCP_FILE_DIR:** Used by Oracle Enterprise Scheduler to store the log and output files. For example, ORACLE_HOME/incident_logs.
- **APPLLOG_DIR:** Location of the PL/SQL log file from Oracle Fusion Applications PL/SQL procedures, on the database server. For example, ORACLE_HOME/incident_logs.
- **OBIEE Backup Directory:** Location of the Oracle Business Intelligence Enterprise Edition dump files.

Note: When specifying an Oracle Business Intelligence Enterprise Edition (OBIEE) backup directory, set it to be a shared directory with read/write permissions for both FUSIONDB hosts.

- **KEYFLEXCOMBFILTER:** Location of the Filter XMLSchema. For example, /tmp.

Secure Enterprise Search

- **Do you have Advanced Compression Option (ACO) License? Yes (Y) or No (N):** Default is No.
- **Do you have Oracle Partitioning option License? Yes (Y) or No (N):** Default is No.

Master and Work Repository

Note: The default values are the **only** valid values. If you change any of these values, the ODI-related provisioning process will not work.

- **Master Repository ID:** Default = 501
- **Supervisor Password:** Enter and confirm your ODI supervisor password.
- **Work Repository Type:** (D) Development or (R). Default = D
- **Work Repository ID:** Default = 501
- **Work Repository Name:** Default = FUSIONAPPS_WREP
- **Work Repository Password:** Default = None. Enter and confirm your ODI supervisor password.

Oracle Transactional BI

- Directory on the database server where Oracle Transactional Business Intelligence import and export files are stored. For example, /tmp.

Activity Graph and Analytics

- **Install Analytics with Partitioning (Y/N):** Default is N.

Click **Next** to continue.

Figure 4–7 Custom Variables Screen

Repository Creation Utility - Step 5 of 8 : Custom Variables

Custom Variables

Enter value for the following custom variables.

Component	Custom Variable	Value
Fusion Applications	Directory on the database machine wh...	DUMP FILE LOCATION
	Directory for the APPLCP_FILE_DIR dire...	INCIDENT LOG LOCATION
	Directory for the APPLLOG_DIR directo...	INCIDENT LOG LOCATION
	Directory for the OBIEE Backup directo...	SHARED OBIEE BACKUP DIRECTORY
Secure Enterprise Search	Directory for the KEYFLEXCOM8FILTER ...	/tmp
	Do you have Advanced Compression ...	N
Master and Work Repository	Do you have Oracle Partitioning option...	N
	Master Repository ID(001)	501
	Supervisor Password	*****
	Confirm Supervisor Password	*****
	Work Repository Type: (D) Developme...	D
	Work Repository ID(001)	501
Oracle Transactional BI	Work Repository Name (WORKREP)	FUSIONAPPS_WREP
	Work Repository Password	*****
	Confirm Work Repository Password	*****
Activity Graph and Analytics	Directory in the database server, wher...	DUMP FILE LOCATION
	Install Analytics with Partitioning (Y/N)	N

Messages:

Help < Back Next > Finish Cancel

10. In the Map Tablespaces screen, click **Next**.
11. In the Summary screen, click **Create**.
12. In the Completion Summary screen, click **Close**.

Note: If you encounter any issues while using the Repository Creation Utility, check the logs at `RCU_HOME/rcu/log`.

Note: Oracle recommends using the database used for identity management to store the Oracle WSM policies. It is therefore expected to use the IM database information for the OWSM MDS schemas, which will be different from the one used for the rest of SOA schemas. To create the required schemas in the database, repeat the steps above using the IM database information, but select only "AS Common Schemas: Metadata Services" in the Select Components screen (Step 7).

4.5 Backing Up the Database

After you have loaded the metadata repository in your database, you should make a backup.

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

Using the Provisioning Process to Install Components for an Enterprise Deployment

This chapter describes the provisioning process that is used to install and configure components specifically required for an enterprise deployment.

For general information about provisioning and installation, see the "Overview" chapter in the *Oracle Fusion Applications Installation Guide*.

This chapter includes the following topics:

- [Section 5.1, "Understanding Provisioning"](#)
- [Section 5.2, "Prerequisites for Using the Provisioning Process"](#)
- [Section 5.3, "Installing Components"](#)
- [Section 5.4, "Configuring Components"](#)
- [Section 5.5, "Performing Post-Provisioning Tasks"](#)

5.1 Understanding Provisioning

Provisioning is the entire set of operations required to install, configure, and deploy applications product offerings from a system point of view. It performs these operations:

- **Install** - operations related to laying down all the component needed to create an Oracle Fusion Applications environment.
- **Configure** - the tailoring of components based on the applications topology, the creating of Managed Server instances and cluster members, and the updating of endpoints and virtual hosts.
- **Deploy** - process that starts the Managed Servers and clusters and facilitates the actual use of product offerings.

Note: Provisioning does not supply users, tenants, or hardware.

For more information about Oracle Fusion Applications architecture, see "Key Oracle Fusion Applications Concepts" in the *Oracle Fusion Applications Administrator's Guide*.

5.2 Prerequisites for Using the Provisioning Process

Before starting the provisioning process, you must do the following:

- Make sure you first install the Oracle Identity Management stack for Oracle Fusion Applications. Follow the instructions in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition)* to install and configure these components.

Keep a record of the configuration details. You must supply them to the Provisioning Wizard when you create your provisioning response file. For more information, see [Section 5.3.2.15, "Identity Management Configuration Screen."](#)

- Make sure you obtain the certificates file from the Oracle Identity Management installation. The installation contains all the Oracle Identity Management certs.
- Make sure all the virtual IPs shown in [Table 3–1 in Chapter 3, "Preparing the Network for an Enterprise Deployment"](#) have been created before you start the provisioning process. (The VIPs are required for the scale-out chapters that follow, and not for provisioning.)
- (Optional) If the user-created user needs to be a superuser, create a user for the superuser (perform these steps on the OIDHOST of the Oracle Identity Management setup):

1. Create a `SuperUser.ldif` file and include the following data:

```
dn: cn=FAAdmin,cn=Users,dc=MyCompany,dc=com
objectclass: top
objectclass: person
objectclass: organizationalPerson
objectclass: inetOrgPerson
objectclass: orclUser
objectclass: orclUserV2
cn: FAAdmin
sn: FAAdmin
description: This user will be provisioned for super admin group
givenname: FAAdmin
orclsamaccountname: FAAdmin
uid: FAAdmin
userpassword: welcome1
```

2. Add the FAAdmin user into the Identity Store of your Oracle Identity Management stack for Oracle Fusion Applications. For example, assuming your Identity Store is in Oracle Internet Directory, run the following command:

```
ldapadd -h idstore.mycompany.com -p 389 -D cn=orcladmin -w password
-c -x -f SuperUser.ldif
```

where

- `idstore.mycompany.com` is the access point of your Identity Store
- `389` is the port configured for non-SSL LDAP traffic
- `password` is the Administrator password

For more information, see "Oracle Access Manager 11g and Oracle Identity Manager 11g for Fusion Applications" and "Extending the Domain to Include Oracle Internet Directory" in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Identity Management (Oracle Fusion Applications Edition)*.

3. Do the following to make the superuser SSO-enabled:
 - a. Create an `inputfile.config` file with following values:

```
IDSTORE_HOST: IDSTORE_HOST
```

```
IDSTORE_PORT: IDSTORE_PORT
IDSTORE_ADMIN_USER: IDSTORE_ADMIN_USER
IDSTORE_USERSEARCHBASE: IDSTORE_USERSEARCHBASE
IDSTORE_GROUPSEARCHBASE: IDSTORE_GROUPSEARCHBASE
PASSWORD_EXPIRY_PERIOD: 7300
```

Note: The value "7300" is an example PASSWORD_EXPIRY_PERIOD.

- b. Run the following command (note that *ORACLE_HOME*, *MW_HOME*, and *JAVA_HOME* need to be set):

```
./idmConfigTool.sh -upgradeLDAPUsersForSSO input_file=inputfile.config
log_level=ALL log_file=upgradeLDAPUsersForSSO.out dump_params=true
```

Note: The `idmConfigTool.sh` script can be found in the Oracle Identity Management installation.

5.3 Installing Components

This section covers the following topics:

- [Section 5.3.1, "Creating the Installation Environment"](#)
- [Section 5.3.2, "Creating a New Provisioning Response File"](#)
- [Section 5.3.3, "Running the Provisioning Commands to Install Components"](#)

5.3.1 Creating the Installation Environment

Oracle Fusion provisioning repositories consist of multiple installers from Oracle Fusion Middleware and Oracle Fusion Applications. In order to run the Fusion provisioning process, these installers must be in a predefined directory structure.

This section includes the following topics:

- [Downloading the Provisioning Repository](#)
- [Installing the Provisioning Framework Bits](#)

5.3.1.1 Downloading the Provisioning Repository

A zipped provisioning repository is included in the Oracle Fusion Applications Product Media Pack. See "Obtaining the Software" in *Oracle Fusion Applications Installation Guide* for instructions on how to get it.

Extract the contents of all the zipped files to the same target directory (*ORACLE_BASE/repository*) that is on a shared/network drive. By default, the installers are located in *repository_location/installers*.

5.3.1.2 Installing the Provisioning Framework Bits

The provisioning framework supplies the components needed to orchestrate the provisioning process. Once set up, this framework retrieves the components and installers silently when they are required.

5.3.1.2.1 Running the Provisioning Installer Run the installer from the directory where you created the provisioning repository. For example: *repository_location/installers/faprov/Disk1*.

Note: If you are running a fresh install or are re-running the installer after cleaning up previously installed products, ensure that no */etc/oraInst.loc* file exists.

To run the installer:

```
>FINHOST1 ./runInstaller
```

When prompted, enter the following JRE/JDK location:

```
repository_location/jdk6
```

Use the screen information in [Table 5–1](#) as a guide when running the installer.

Note: In the case of a clean host, that is, one where the */etc/oraInst.loc* file does not exist:

- The oraInventory creation panels will display prior to the start of the Provisioning Wizard
 - A confirmation dialog asking you to execute *oracleRoot.sh* will display at the end of the installation
 - On the Specify Inventory Directory screen, specify the location as *ORACLE_BASE/oraInventory*
-

Table 5–1 Provisioning Installer Screens

Screen Name	Description
Welcome	The standard Welcome screen is read-only and appears each time you start the provisioning framework installer. No action is required. Click Next to continue.
Prerequisite Checks	Analyzes the host computer to ensure that specific operating system prerequisites have been met. If any prerequisite check fails, the screen displays a short error message at the bottom. Fix the error and click Retry. If you want to ignore the error or warning message, click Continue. Click Abort to stop the prerequisite check process for all components. Click Next to continue.
Specify Installation Location	Specify a location where you want to install the provisioning framework (<i>ORACLE_BASE/repository</i>). This is the location where the Provisioning Wizard and the start commands for provisioning (<i>runProvisioning</i>) are installed. The Oracle Fusion Applications Provisioning framework must be installed on a shared disk in a location that is accessible to all hosts to be provisioned. Click Next to continue.

Table 5–1 (Cont.) Provisioning Installer Screens

Screen Name	Description
Installation Summary	Summarizes the selections you have made during this installation session. To change this configuration before installing, select one of the screens from the left navigation pane. Click Save to create a text file (response file) to use if you choose to perform the same installation at a later date. Click Install to continue installing this configuration.
Installation Progress	The progress indicator shows the percentage of the installation that is complete and indicates the location of the installation log file. Click Next when the progress indicator shows 100 percent.
Installation Complete	Summarizes the installation just completed. If you want to save the details to a text file, click Save and indicate a directory where you want to save the file. Click Finish to dismiss the screen and exit the installer.

/provisioning Directory Structure:

After installing the provisioning framework, the directories in `ORACLE_BASE/repository/provisioning` should be the following:

```
ant bin labelInfo.txt lib provisioning-build provisioning-plan
template util
```

Note: Installation logs are located in the `ORACLE_BASE/oraInventory` directory.

Move or copy the directories and files from the `repository_location` to `ORACLE_BASE/repository`:

```
FINHOST1> mv repository_location/* ORACLE_BASE/repository
```

5.3.2 Creating a New Provisioning Response File

Before provisioning the Oracle Fusion Applications enterprise deployment environment, you must generate the provisioning response file, which will serve as the input for the actual provisioning process. You generate the provisioning response file by completing a number of wizard interview screens to collect the configuration details for your provisioning response file and save the file in a location that is accessible to the provisioning installers. Be sure to make a note of the provisioning response file name and location, as you must supply these when you run the physical installation.

Before launching the provisioning wizard, set `JAVA_HOME` and `PATH`. For example:

```
FINHOST1> export JAVA_HOME=ORACLE_BASE/repository/jdk6
```

```
FINHOST1> export PATH=$JAVA_HOME/bin:$PATH
```

Launch the provisioning wizard from any host in the enterprise deployment environment:

```
FINHOST1> cd ORACLE_BASE/repository/provisioning/bin
```

```
FINHOST1> ./provisioningWizard.sh
```

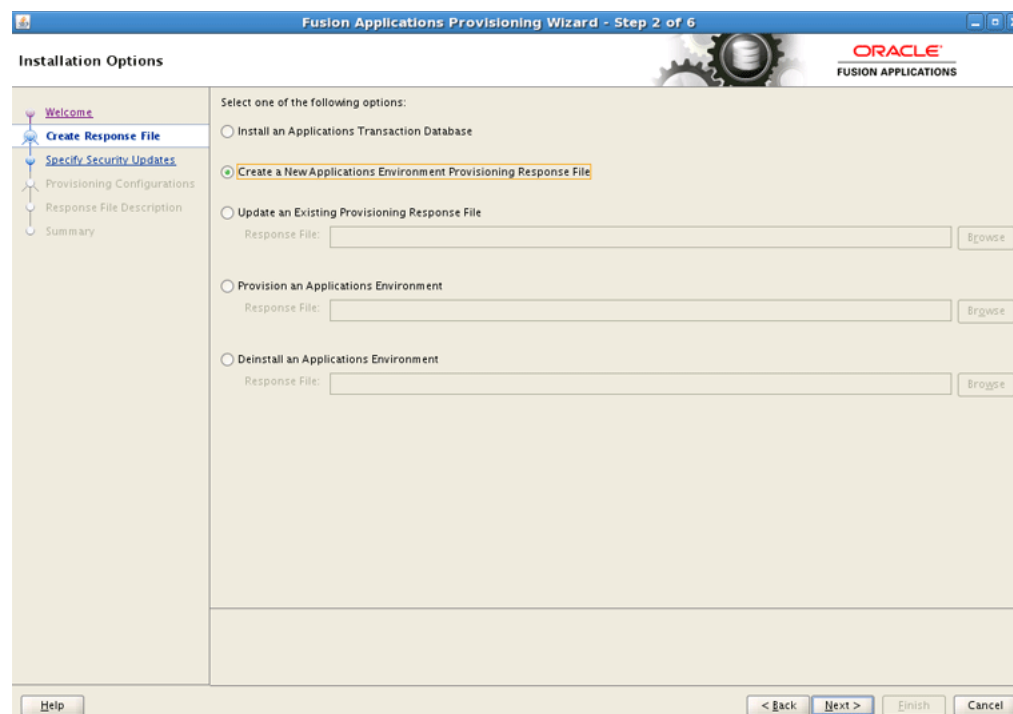
The Oracle Fusion Applications Provisioning Wizard is launched and the Welcome screen displays. The screen is read-only and displays each time you start the Wizard. Click **Next**.

5.3.2.1 Installation Options Screen

In this screen, shown in [Figure 5–1](#), select only the following task from the list of options:

Create a New Applications Environment Provisioning Response File - create a provisioning response file for a new Oracle Fusion Applications environment.

Figure 5–1 Installation Options Screen



Click **Next** to continue.

5.3.2.2 Specify Security Updates Screen

In this screen, you can set up a notification preference for security-related updates and installation-related information from Oracle Support.

- **Email** - specify your email address to have updates sent by this method.
- **I wish to receive security updates via My Oracle Support** - specify your **My Oracle Support Password** to have updates posted to your account.

Click **Next** to continue.

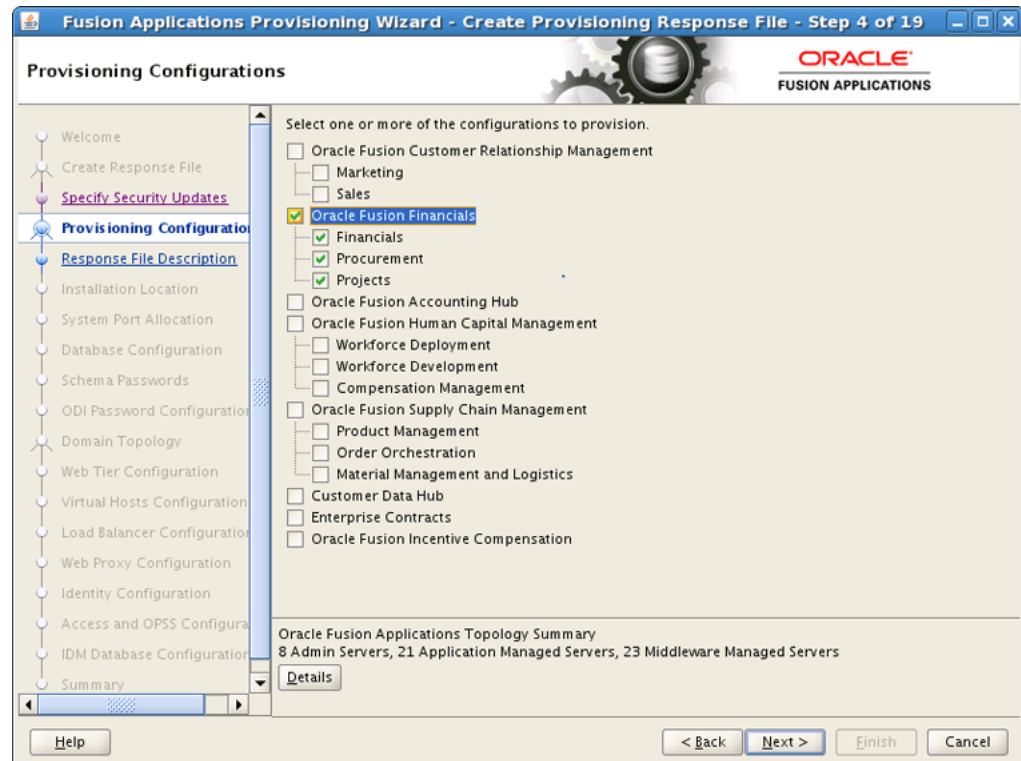
5.3.2.3 Provisioning Configurations Screen

This screen, shown in [Figure 5–2](#), enables you to select the Oracle Fusion Financials options to configure.

Select only the Oracle Fusion Financials option, shown in [Figure 5–2](#). When selected, the Financials, Procurement, and Projects options are automatically selected.

The information in the message pane displays a cumulative estimate of the number of Managed Servers made available based on the offerings you selected. Click **Details** to see a breakdown of servers by domain.

Figure 5–2 Provisioning Configurations Screen



Click **Next** to continue.

5.3.2.4 Response File Description Screen

This *optional* screen lets you enter descriptive information to identify this response file, or create another version. This information becomes part of the summary document, and is listed under the Global settings on the **Summary** screen. It does not affect the content of your response file.

Update the response file name and click **Next** to continue.

5.3.2.5 Installation Location Screen

In this screen, shown in [Figure 5–3](#), specify credentials for the node manager and supply the location of the various directories required for installation and configuration actions.

Use the values shown in the screen for your installation.

- **Node Manager Credentials** options - Add the values for the Node Manager credentials, which are used by Node Manager to start the Managed Server.
- **Installers Directory Location** - Specify the location of the repository you created. For example, `ORACLE_BASE/repository`.
- **Oracle Fusion Application Home** - The root directory of all Oracle Fusion Applications and Oracle Fusion Middleware products. Typically, this location is on a shared disk, `ORACLE_BASE/products`.

- **Application Configuration Directory** - Specify the path of the root directory where you want to write and manage the configuration files for all the domains, and from where the Administration Servers are started. Typically, this location is on a shared disk, `ORACLE_BASE/config`. (Note that `ORACLE_BASE/config` should be empty.)
- **Enable Local Application Configuration** - Enable this option. When enabled, all the Managed Servers will run locally; only the Administration Server will run from the shared disk. Provisioning will run pack and unpack, and will create local domain directories.
- **Local Application Config Directory** - Specify a local-drive location, for example, `/u02/local/oracle/config`. This field is required if you selected **Enable Local Application Configuration**.
- **Font Directory** - Enter the directory where the TrueType fonts are installed. The location varies on different operating systems, but is typically found at `/usr/share/X11/fonts/TTF`.
- **Default IDM Configuration Using IDM Properties file** - Check this box if you want the values on the **Identity Management Configuration** and the **Access and Policy Management Configuration** screens to default to the values in the Oracle Identity Manager properties file. Provide the full path to the file.
- **Oracle Business Intelligence Repository Password options** - Specify and confirm a password to allow access to the metadata repository (RPD) for both Oracle Business Intelligence Applications and Oracle Transactional Business Intelligence.

Figure 5–3 Installation Location Screen

The screenshot shows the 'Fusion Applications Provisioning Wizard - Create Provisioning Response File - Step 6 of 19'. The main window is titled 'Installation Location'. On the left, a navigation pane lists steps: Welcome, Create Response File, Specify Security Updates, Provisioning Configurations, Response File Description, **Installation Location** (selected), System Port Allocation, Database Configuration, Schema Passwords, ODI Password Configuration, Domain Topology, Web Tier Configuration, Virtual Hosts Configuration, Load Balancer Configuration, Web Proxy Configuration, Identity Configuration, Access and OPSS Configuration, IDM Database Configuration, and Summary. The main content area is divided into sections:

- Node Manager Credentials:**
 - User Name:
 - Password:
 - Confirm Password:
- Installation and Configuration:**
 - Installers Directory Location:
 - Oracle Fusion Application Home:
 - Application Configuration Directory:
 - ☒ **Enable Local Application Configuration**
 - Local Application Config Directory:
- Middleware Dependencies:**
 - Font Directory:
 - ☐ **Default IDM Configuration Using IDM Properties file**
 - IDM Properties file:
- Oracle Business Intelligence Repository Password:**
 - RPD Password:
 - Confirm Password:

At the bottom, there are buttons: Help, Save, < Back, **Next >** (highlighted), Finish, and Cancel.

Click **Next** to continue.

5.3.2.6 System Port Allocation Screen

In this screen, shown in [Figure 5–4](#), accept the **Applications Base Port** value or enter a custom value. If you change the base port default, you must reset the domain port ranges accordingly. Port ranges must not overlap and must be stated as ascending values.

High and low port ranges are assigned by default to each product family per domain in the **Application Domain Port Ranges** list. The default range allotment for each product family is 399, with each family's range arranged in ascending order.

The **Other Ports** section contains the default value for the Node Manager port.

Figure 5–4 System Port Allocation Screen

Click **Next** to continue.

5.3.2.7 Database Configuration Screen

In this screen, shown in [Figure 5–5](#), click **Add** to create a line in the table for each instance in this database. Select a row and click **Remove** if you need to revise the table. Specify the following information for each instance:

- **User Name (SYSDBA Role)** - the user name of the sysdba role. This user name is used to upgrade schemas during the configuration phase. Note that the sysdba fields are not validated, so ensure that you enter the correct values.
- **Password** - the password of the sysdba role.
- **Host Name** - the name of the Oracle RAC host for each instance.
- **Port** - listening port of the database.
- **Instance Name** - the Oracle RAC database instance name

Figure 5–5 Database Configuration Screen

Database Configuration

Choose the option that describes the Oracle Fusion Applications transaction database configuration.

☐ Single-instance Database

User Name (SYSDBA Role):

Password:

Host Name:

Port: 1521

Service Name: fusion

☒ Real Application Clusters Database

User Name (SYSDBA Role): SYSDBA ROLE

Password: *****

Service Name: fin.mycompany.com

Host Name	Port	Instance Name
FUSIONDBHOST1	1521	FADB1
FUSIONDBHOST2	1521	FADB2

Add Remove

Help Save < Back Next > Finish Cancel

Click **Next** to continue.

5.3.2.8 Schema Passwords Screen

In this screen, shown in [Figure 5–6](#), enter the same password for all the accounts or, if there are different passwords for each account, select **Use a different password for each account** and enter the passwords.

Note: It is recommended to use a separate password for each account in the production deployment.

Figure 5–6 Schema Passwords Screen

Fusion Applications Provisioning Wizard - Create Provisioning Response File - Step 9 of 19

Schema Passwords

The transaction database contains pre-loaded schemas required for runtime execution. Specify the passwords for these accounts. Passwords can contain alphabetic, numeric and these special characters (\$, #, _).

☒ Use the same password for all accounts

Password:

☐ Use a different password for each account

Account	Password
FUSION	
FUSION_DYNAMIC	
FUSION_RUNTIME	
FUSION_APM	
FUSION_AQ	
FUSION_BI	
FUSION_DQ	
FUSION_ODI_STAGE	

Account	Password
FUSION_ORA_ESS	
CRM_FUSION_MDS_SOA	
FIN_FUSION_MDS_SOA	
HCM_FUSION_MDS_SOA	
QIC_FUSION_MDS_SOA	
PPC_FUSION_MDS_SOA	
PPI_FUSION_MDS_SOA	
SCM_FUSION_MDS_SOA	

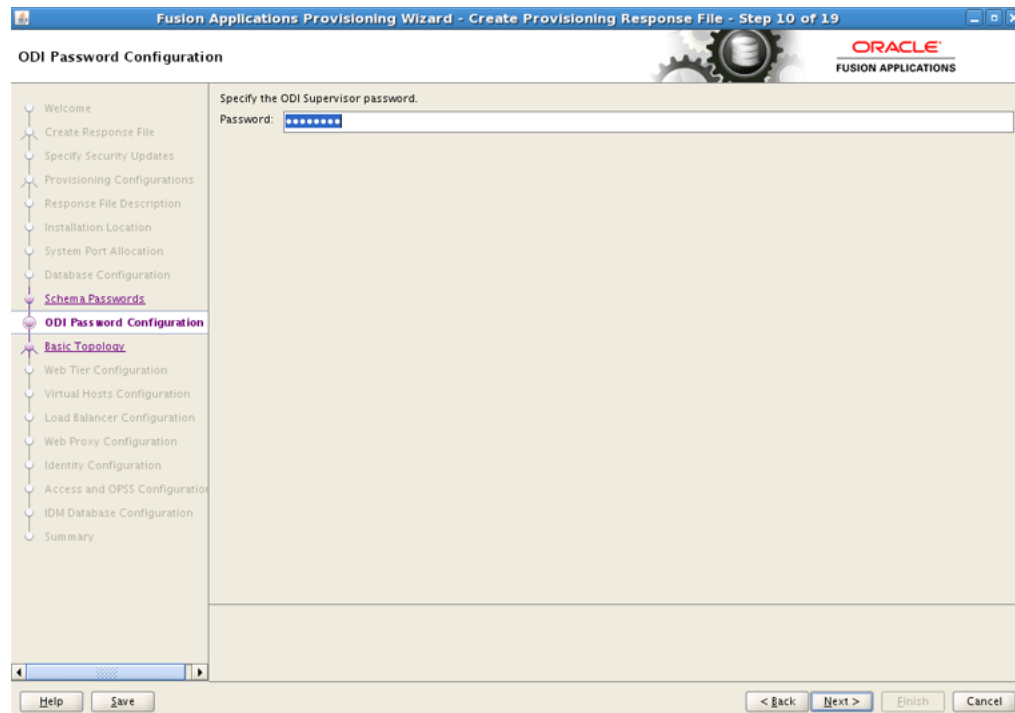
Help Save < Back Next > Finish Cancel

Click **Next** to continue.

5.3.2.9 ODI Password Configuration Screen

In this screen, shown in [Figure 5–7](#), enter the Oracle Data Integrator Supervisor Password that was used when the Oracle Fusion Middleware Metadata Repository was loaded into the Oracle RAC database (see [Figure 4–7](#) in [Section 4.4, "Loading the Oracle Fusion Applications Repository into the Oracle RAC Database"](#)).

Click **Next** to continue.

Figure 5–7 ODI Password Configuration

5.3.2.10 Domain Topology Configuration Screen

In this screen, shown in [Figure 5–8](#), determine the flow for the remaining wizard interview screens.

- **One host for all domains** - select this option to specify a **Host Name** if there is only one host and the ports are not changing.
- **One host per domain** - select this option if the domains are to be split among several machines. Use the dropdown list to select a **Host Name** for each application domain to be created.
- **One host per application and middleware component** - select this option when there are different hosts and ports to be modified.

Figure 5–8 Domain Topology Configuration Screen

Domain Topology Configuration

Select one of the following domain topology options:

☒ One host for all domains
Host Name:

☐ One host per domain

Application Domain	Host Name
Common	
Customer Relationship Management	
Financials	
Human Capital Management	
Procurement	
Projects	
Supply Chain	
Business Intelligence	

☐ One host per application and middleware component

Help Save < Back Next > Finish Cancel

5.3.2.11 Web Tier Configuration Screen

This screen, shown in Figure 5–9, allows you to create virtual hosts on a single Oracle Web Tier that are either port-based or name-based for each product family domain that is created during installation. Specify an internal and an external port. The values assigned during installation are derived from the default HTTP port you name on this screen.

Web Tier

- **Install Web Tier in DMZ** - select this option if you set up a separate host for web tier installation. This host is set up as a demilitarized zone (DMZ), which does not have access to the shared file system. It cannot be used for any other host deployed, regardless of domain.
- **Host** - enter the name of the host where the Oracle HTTP Server will be installed and configured.
- **Virtual Host Mode** - select **IP-based** to create new DNS entries to use as virtual hosts. For example, `fin.mycompany.com`.
- **Domain Name** - specify a domain name (only if you select a name-based virtual host). For example, `mycompany.com`.
- **HTTP Port** - default port for the Web Tier. Should not require operating system administrator privileges. Use the default values.
- **HTTP (SSL) Port** - secure port for the Web Tier. Should not require operating system administrator privileges. Use the default values.

Figure 5–9 Web Tier Configuration Screen

Click **Next** to continue.

5.3.2.12 Virtual Hosts Configuration Screen

This screen, shown in [Figure 5–10](#), contains the configuration details for the domains on the virtual hosts.

Specify the following information for each application domain listed:

- **Internal Name** - the host name or IP address where the Webtier listens on the internal virtual host for this domain.
- **Internal Port** - port for this internal virtual host. Should be visible only from inside the firewall.
- **External Name** - the host name or IP address for the external virtual host for this product family or middleware dependency. The host:port should be visible from outside the firewall.
- **External Port** - port to be used for this external virtual host. The host:port should be visible from outside the firewall.

If you selected **Name-based** on the Web Tier Configuration screen, specify the following information for each domain listed:

- **Internal.Name** - the DNS name for this internal virtual host. For example, for Financials, the name might be *fin-internal*.
- **External.Name** - the DNS name for this external virtual host. For example, for Financials, the name might be *fin*.

If you selected **Port-based** on the Web Tier Configuration screen, specify the following information for each domain listed:

- **Internal Port** - the port that is visible only from inside the firewall for this domain.

- **External Port** - the port that is visible from outside the firewall for this domain.

Figure 5–10 Virtual Hosts Configuration Screen

Specify the configuration settings for the virtual hosts required by Oracle Fusion Applications.

IP-based Virtual Hosts Configuration

Application Domain	Internal Name	Internal Port	External Name	External Port
Financials	WEBHOST1.mycompany.com	10603	WEBHOST1.mycompany.com	10604
Projects	WEBHOST1.mycompany.com	10605	WEBHOST1.mycompany.com	10606
Procurement	WEBHOST1.mycompany.com	10607	WEBHOST1.mycompany.com	10608
Procurements Supplier Portal	WEBHOST1.mycompany.com	10609	WEBHOST1.mycompany.com	10610
Common	WEBHOST1.mycompany.com	10613	WEBHOST1.mycompany.com	10614
Customer Relationship Management	WEBHOST1.mycompany.com	10615	WEBHOST1.mycompany.com	10616
Supply Chain	WEBHOST1.mycompany.com	10617	WEBHOST1.mycompany.com	10618
Human Capital Management	WEBHOST1.mycompany.com	10619	WEBHOST1.mycompany.com	10620
Business Intelligence	WEBHOST1.mycompany.com	10621	WEBHOST1.mycompany.com	10622

Help Save < Back Next > Finish Cancel

Click **Next** to continue.

5.3.2.13 Load Balancer Configuration Screen

This screen, shown in [Figure 5–11](#), enables you to distribute workload evenly across two or more hosts, network links, CPUs, hard drives, or other resources. Check **Load Balancing Enabled** to take advantage of this feature, and specify:

- **Internal Load Balancer Configuration** - the host and port for the internal Virtual IP (VIP).
- **External Load Balancer Configuration** - the host and port for external Virtual IP (VIP). It must have a publicly available address to be usable.

If you want to stop creating this response file and resume at a later date, click **Save**. This action creates a partial response file. A partial response file cannot be used to provision an environment.

Figure 5–11 Load Balancer Configuration Screen

Load Balancer Configuration

☒ Load Balancing Enabled

Internal Load Balancer Configuration

	Internal VIP Host	Internal VIP Port
Financials	fininternal.us.oracle.com	7777
Projects	prjinternal.us.oracle.com	7777
Procurement	prcinternal.us.oracle.com	7777
Procurement Supplier Portal	prcsupplierportal-internal.us.oracle.com	7777
Common	commoninternal.us.oracle.com	7777
Customer Relationship Management	crminternal.mycompany.com	7777
Supply Chain	scminternal.us.oracle.com	7777
Human Capital Management	hcminternal.us.oracle.com	7777
Business Intelligence	biinternal.us.oracle.com	7777

External Load Balancer Configuration

	External VIP Host	External VIP Port
Financials	finexternal.us.oracle.com	443
Projects	prjexternal.us.oracle.com	443
Procurement	prcexternal.us.oracle.com	443
Procurement Supplier Portal	prcsupplierportal-external.us.oracle.com	443
Common	commonexternal.us.oracle.com	443
Customer Relationship Management	crmexternal.us.oracle.com	443
Supply Chain	scmexternal.us.oracle.com	443
Human Capital Management	hcmexternal.us.oracle.com	443
Business Intelligence	biexternal.us.oracle.com	443

Help Save < Back Next > Finish Cancel

Click **Next** to continue.

5.3.2.14 Web Proxy Configuration Screen

This screen, shown in [Figure 5–12](#), allows you to create Proxy Settings to enable users who want to use a proxy server to connect to the Internet.

Figure 5–12 Web Proxy Configuration Screen

5.3.2.15 Identity Management Configuration Screen

In these screens, shown in [Figure 5–13](#) and [Figure 5–14](#), enter the **Identity Management Configuration** parameters for the identity management infrastructure associated with this environment.

- **Super User Name** - enter the name of an existing user that should be granted administrator and functional setup privileges.
- **Create Administrators Group** - indicate whether you created an "Administrators" group, whose members have specialized privileges for all Oracle Fusion Middleware components.
- **Create Monitors Group** - indicate whether you created a "Monitors" group, whose members have read-only administrative privileges to Oracle WebLogic domains.
- **Create Operators Group** - indicate whether you created an "Operators" group, whose members have Monitors privileges to Oracle WebLogic domains.
- **Identity Store Server Type** - indicate the type of identity store you set up: Oracle Internet Directory (OID) or Oracle Virtual Directory (OVD).

Important: If the Oracle Identity Manager being used is in the form of an Oracle Identity Manager enterprise deployment, select the "Oracle Virtual Directory" option.

- **Use SSL to Communicate With Identity Store** - this feature is not enabled in this release.
- **Identity Store Host** - enter the host or DNS name for your identity store LDAP service. (The value can be the Load Balancer host of the Oracle Identity Management enterprise deployment setup.)

- **Identity Store Port** - port assigned to the identity store.
- **Identity Store Secure Port** - the SSL port for the identity store.
- **Identity Store User DN** - enter the Distinguished Name of the user you set up with read-write access to the LDAP.
- **Identity Store Password** - enter the password you set up for the user with read-write access to the LDAP.
- **Identity Store Read-Only User DN** - the Distinguished Name of the user with read-only access to the Identity Store LDAP.
- **Identity Store Read-Only Password** - enter the password you set up for the identity store read-only user.
- **Identity Store User Name Attribute** - the type of user name attribute you configured in the identity store. Valid values are: user ID (uid), common name (CN), or email address.
- **Identity Store User Base DN** - enter the root Distinguished Name assigned to the upload of applications user data. This is the root for all the user data in your identity store.
- **Identity Store Group Base DN** - enter the root Distinguished Name for all the group data in your identity store.
- **OIM Admin Server Host** - enter the name of the host where the OIM Administration Server is installed. (This value can be either the host name or the VIP name of host.)
- **OIM Admin Server Port** - the port where the OIM Administration Server listens.
- **OIM Administrator User Name** - enter the Distinguished Name you set up as the OIM administrator.
- **OIM Administrator Password** - enter the password you set up for the OIM administrator.
- **OIM Managed Server Host** - enter the virtual or real host name of the Oracle Identity Manager Managed Server where SPML callback and other OIM services are running. (This value can be either the host name or the VIP name of host.)
- **OIM Managed Server Port** - enter the virtual or real port where the Oracle Identity Manager Managed Server listens.
- **Use SSL to communicate with OIM HTTP Endpoint** - select this option if the endpoint host is SSL-enabled. (This option is currently not available.)
- **OIM HTTP Internal Endpoint URL** - the access point on the Oracle HTTP Server for Oracle Identity Manager services in an Oracle Identity Management enterprise deployment, or the Oracle Identity Manager Managed Server access point for a non-enterprise deployment. This URL is used for deployment.

Enter the http termination address of Oracle Access Manager. Terminates at either a load balancer or the Oracle HTTP Server.
- **OIM HTTP(S) External Endpoint URL** - the access point to use for taxonomy. This is not used for deployment. Note that a non-secure connection is used unless you provide an https URL.

Figure 5–13 Identity Management Configuration Screen (1)

Fusion Applications Provisioning Wizard - Create Provisioning Response File - Step 16 of 19

Identity Management Configuration

Configure Oracle Fusion Applications to integrate with your existing Oracle Identity Management environment.

Identity Management Configuration

Super User Name: SUPERUSER

☒ Create Administrators Group

☒ Create Monitors Group

☒ Create Operators Group

Identity Store Server Type: Oracle Internet Directory

☐ Use SSL to communicate with Identity Store

Identity Store Host: idstore.mycompany.com

Identity Store Port: 3060

Identity Store Secure Port: 3131

Identity Store User DN: cn=USERNAME,dc=mycompany,dc=com

Identity Store Password: *****

Identity Store Read-Only User DN: cn=READONLYUSERNAME,dc=mycompany,dc=com

Identity Store Read-Only Password: *****

Identity Store User Name Attribute: uid

Identity Store User Base DN: cn=Users,dc=mycompany,dc=com

Identity Store Group Base DN: cn=Groups,dc=mycompany,dc=com

OIM Admin Server Host: oim.mycompany.com

OIM Admin Server Port: 7004

OIM Administrator User Name: OIM ADMIN USER

Help Save < Back Next > Finish Cancel

Figure 5–14 Identity Management Configuration Screen (2)

Fusion Applications Provisioning Wizard - Create Provisioning Response File - Step 16 of 19

Identity Management Configuration

Identity Store Server Type: Oracle Internet Directory

☐ Use SSL to communicate with Identity Store

Identity Store Host: idstore.mycompany.com

Identity Store Port: 3060

Identity Store Secure Port: 3131

Identity Store User DN: cn=USERNAME,dc=mycompany,dc=com

Identity Store Password: *****

Identity Store Read-Only User DN: cn=READONLYUSERNAME,dc=mycompany,dc=com

Identity Store Read-Only Password: *****

Identity Store User Name Attribute: uid

Identity Store User Base DN: cn=Users,dc=mycompany,dc=com

Identity Store Group Base DN: cn=Groups,dc=mycompany,dc=com

OIM Admin Server Host: oim.mycompany.com

OIM Admin Server Port: 7004

OIM Administrator User Name: OIM ADMIN USER

OIM Administrator Password: *****

OIM Managed Server Host: oim.mycompany.com

OIM Managed Server Port: 7004

OIM HTTP Internal Endpoint URL: http://oiminternal.mycompany.com:7777

OIM HTTP(S) External Endpoint URL: https://oimexternal.mycompany.com:443

Help Save < Back Next > Finish Cancel

Click **Next** to continue.

5.3.2.16 Access and Policy Management Configuration Screen

Access and Policy Management Configuration provides identity administration and security functions such as Single Sign-On and policy management. In these screens, shown in [Figure 5–15](#) and [Figure 5–16](#), supply the following parameters to integrate with your existing Oracle Identity Management environment:

- **OAM Administrator User Name** - enter the name you assigned this user when you installed Oracle Access Manager.
- **OAM Administrator Password** - enter the password you assigned this user when you installed Oracle Access Manager.
- **OAM AAA Server Host** - enter the name of the proxy host where Oracle Access Manager is installed. (This value can be either the host name or the VIP name of host.)
- **OAM AAA Server Port** - the port number for the Oracle Access Manager listener on the OAM proxy host..
- **Access Server Identifier** - name used to identify the Oracle Access Server.
- **Enable Second Primary Oracle Access Manager** - select this check box to name a second Primary Oracle Access Manager for high availability.
- **Second Access Server Identifier** - enter the name of the second Primary Oracle Access Manager Server.

Note: After connecting to the primary access server, provisioning is able to get the secondary access server connection information.

- **OAM Security Mode** - enter the OAM transport security mode that you set up for this access server when you installed Oracle Access Manager. Values are Simple or Open.
- **OAM Simple Mode Passphrase** - enter the passphrase that you set up to secure the communication with the OAM Server. Required only if the mode is specified as Simple.
- **Webgate Password/Confirm Password** - specify a password for the Resource WebGate. It must contain at least eight alphanumeric characters and at least one digit or punctuation mark. Re-type to Confirm the password. If seeding of security data is disabled, the password must be the existing WebGate password.
- **Default to Identity Store** - the default values of this section depend on whether this field is enabled. If the checkbox is unchecked, which is the default, the **OPSS Policy Store Host**, **OPSS Policy Store Read-Write User Name** and **OPSS Policy Store Password** fields are empty by default and do not inherit values from your identity store.
- **Use SSL to communicate with OPSS Policy Store** - this feature is not enabled in this release.
- **OPSS Policy Store Host** - enter the host name for OID where Oracle Platform Security Services (OPSS) policies are to be seeded. (The value can be the Load Balancer host of the Oracle Identity Management enterprise deployment setup.)
- **OPSS Policy Store Port** - number of the OID port for OPSS policy store.
- **OPSS Policy Store Secure Port** - the secure port for OID.

- **OPSS Policy Store Read-Write User Name** - enter the Distinguished Name of the user that you set up with write privileges to the OPSS policy store.
- **OPSS Policy Store Password** - enter the password that you set up for the OPSS policy store user with read-write privileges.
- **OPSS Policy Store JPS Root Node** - enter the Distinguished Name of the node that you set up to be used as the OPSS policy root.
- **Create OPSS Policy Store JPS Root Node** - enabled only if the **Enable Seeding of Security Data** checkbox on the Identity Management Configuration screen is selected. Select this option if you want to create the OPSS JPS Root Node.
- **IDM Keystore File** - enter the location of the JKS keystore containing the certificates for the Oracle Identity Management components.
- **IDM Keystore Password** - enter the password that you set up for the IDM Keystore File.

Figure 5–15 Access and Policy Management Configuration Screen (1)

Fusion Applications Provisioning Wizard - Create Provisioning Response File - Step 17 of 19

Access and Policy Management Configuration

Configure Oracle Fusion Applications to integrate with your existing Oracle Identity Management environment.

Oracle Access Manager Configuration

OAM Admin Server Host: oam-admin-host

OAM Admin Server Port: 14000

OAM Administrator User Name: OAM-ADMIN-USERNAME

OAM Administrator Password: *****

OAM AAA Server Host: oamhost1.mycompany.com

OAM AAA Server Port: 6021

Access Server Identifier: aaa1

☒ Enable Second Primary Oracle Access Manager

Second Access Server Identifier: aaa2

OAM Security Mode: Simple

OAM Simple Mode Passphrase: *****

Webgate Password: *****

Confirm Webgate Password: *****

Oracle Platform Security Services Configuration

☐ Default to Identity Store

☐ Use SSL to communicate with OPSS Policy Store

OPSS Policy Store Host: polycystore.mycompany.com

OPSS Policy Store Port: 3060

OPSS Policy Store Secure Port: 3131

Buttons: Help, Save, < Back, Next >, Finish, Cancel

Figure 5–16 Access and Policy Management Configuration Screen (2)

Click **Next** to continue.

5.3.2.17 IDM Database Configuration Screen

In this screen, shown in [Figure 5–17](#), enter the configuration details you specified when you installed the database for the Oracle Identity Manager (OIM).

Select **Real Application Clusters Database** if you have installed an OIM database based on Oracle Real Application Clusters (Oracle RAC). Specify the **Service Name**.

To identify the Oracle RAC instances, click **Add** to create a new row in the table. To delete a row, select it and click **Remove**. Enter the following information for each instance:

- **Host Name** - the name of the Oracle RAC host where you have installed the OIM database. In this field, you select an existing host or enter a new one. As you enter values for a new host, the list of hosts is populated with the new information.
- **Port** - listening port of the RDBMS.
- **Instance Name** - the Oracle RAC database instance name

Specify the database schema and password used to store the Metadata Service (MDS) Repository data for Oracle Web Services Policy Manager.

- **Schema Owner** - the MDS schema in the OIM database that is used by Oracle Web Services Policy Manager.
- **Schema Owner Password** - the password for the MDS schema.

Figure 5–17 IDM Database Configuration Screen

Fusion Applications Provisioning Wizard - Create Provisioning Response File - Step 18 of 19

IDM Database Configuration

Choose the option that describes the Oracle Identity Management database configuration.

☐ Single-instance Database

Host Name:

Port:

Service Name:

☒ Real Application Clusters Database

Service Name:

Host Name	Port	Instance Name
IDMDBHOST1	1521	IDMDB1
IDMDBHOST2	1521	IDMDB2

[Add](#) [Remove](#)

Specify the database schema and password used to store MDS data for Oracle Web Services Policy Manager

Schema Owner:

Schema Owner Password:

[Help](#) [Save](#) [< Back](#) [Next >](#) [Finish](#) [Cancel](#)

Click **Next** to continue.

5.3.2.18 Summary Screen

Review the information on this screen. If it is not what you expected or intended, click **Back** to return to the interview flow screen that needs to be changed, or click the name of the screen in the left navigation pane.

Descriptive information for this response file (if any) and database connection details are displayed under **Global Settings**. Each *product family Domain* to be created is listed along with the configuration details you have previously entered.

If you are satisfied with the information as displayed, specify the following information:

- **Provisioning Response File Name** - the executable file that contains the configuration details of this provisioning response file.
- **Provisioning Summary** - a text document that summarizes the details of this provisioning response file. You cannot use this file to execute the response file.
- **Directory** - the directory path to the location where you save the response file and the summary document.

Make a note of the name and location where you saved the executable file. You must supply this information to the Installation Wizard for other options.

Click **Finish** to save the `file_name.rsp` and `provisioning.summary` files to `ORACLE_BASE/repository/provisioning/bin`.

5.3.3 Running the Provisioning Commands to Install Components

The provisioning commands that install components perform the following tasks:

- [Set up WEBHOST1](#)

- [Set up the debug flag](#)
- [Run the pre-verify phase](#)
- [Run the installation phase](#)

Prerequisites for running the provisioning commands

Before running the provisioning commands which run the ant targets (preverify, install, and so on), do the following:

- Check the latest Oracle Fusion Applications release notes for any known workarounds.
- Ensure that the preverify target is passed before you move on to other targets.
- Ensure that all commands with ant targets say "Build Successful" when they pass.
- Set the `JAVA_HOME` variable to `ORACLE_BASE/repository/jdk6`.
- On `FINHOST1` and `WEBHOST1`, create the `/etc/oraInst.loc` file with the following entries:

```
inventory_loc=ORACLE_BASE/oraInventory
inst_group=usergroup
```

- For commands that fail, use the following location to debug:

```
ORACLE_BASE/products/logs/provisioning/FINHOST1/
runProvisioning-targetname.log
```

Note: In the provisioning commands that follow, the `-override` parameter takes the option `override.properties`. The `override.properties` file contains the changes that are required for `responseFile` values.

Note: If for any reason you need to run any target again, run the following:

```
./runProvisioning.sh -responseFile ./file_name.rsp -override
./overrides.properties -target cleanup-targetname
```

```
./runProvisioning.sh -responseFile ./file_name.rsp -override
./overrides.properties -target restore-targetname
```

Then run the target again.

Task 1 Set up `WEBHOST1`

For this task, `WEBHOST1` is the host you configured in [Figure 5-9](#), and `WEBHOST1` and `FINHOST1` do not have a common shared storage. From `FINHOST1`, copy `ORACLE_BASE/repository` to `ORACLE_BASE` on `WEBHOST1`.

Be sure to maintain the same directory structure on `WEBHOST1`.

Task 2 Set up the debug flag

Run the following commands:

- On `FINHOST1`: `export DEBUG_PROVISIONING=true`

- On **WEBHOST1**: `export DEBUG_PROVISIONNING=true`

Task 3 Run the pre-verify phase

Run the following commands from `ORACLE_BASE/repository/provisioning/bin`:

- On **FINHOST1**: `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target preverify`

Note: If pre-verify fails when validating Oracle Access Manager against Oracle Identity Manager in an enterprise deployment environment, do the following:

1. On **FINHOST1**, change directory to `ORACLE_BASE/config/phaseguards/`.
2. Delete the `FAILED.grd` file on **FINHOST1** and add `STARTED.grd` and `COMPLETED.grd` files for **WEBHOST1** on **FINHOST1**:

```
touch preverify-FINHOST1-STARTED.grd
touch preverify-FINHOST1-COMPLETED.grd
touch preverify-WEBHOST1-STARTED.grd
touch preverify-WEBHOST1-COMPLETED.grd
```

- On **WEBHOST1**: `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target preverify`

Task 4 Run the installation phase

Run the following commands from `ORACLE_BASE/repository/provisioning/bin`:

- On **FINHOST1**: `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target install`

Note: If the install target fails for Oracle Identity Manager split domain in an enterprise deployment environment, update the following lines in the *ORACLE_BASE/repository/provisioning/provisioning-build/webgate-build.xml* file:

- **Change**

```
<echo message="oam_admin_server=  
http://${provisioning.include.idm.oim.adminserver.host.name}:  
${provisioning.include.idm.oim.adminserver.port}" />
```

to

```
<echo message="oam_admin_server=  
http://${provisioning.include.oam.admin.server.host.name}:  
${provisioning.include.oam.admin.server.port}" />
```

- **Change**

```
<arg value="oam_admin_server=  
http://${provisioning.include.idm.oim.adminserver.host.name}:  
${provisioning.include.idm.oim.adminserver.port}" />
```

to

```
<arg value="oam_admin_server=  
http://${provisioning.include.oam.admin.server.host.name}:  
${provisioning.include.oam.admin.server.port}" />
```

- **On *WEBHOST1*:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target install`

Note: If the relative path for the response file (*./file_name.rsp*) and override properties (*./override.properties*) does not work, give a fully qualified path instead.

5.4 Configuring Components

The provisioning commands that configure components perform the following tasks:

- [Run the pre-configure phase](#)
- [Run the configure phase](#)
- [Run the configure secondary phase](#)
- [Run the post-configure phase](#)
- [Run the start-up phase](#)
- [Run the validate phase](#)
- [Configure email servers](#)

Note: If any target fails and you have to run the configure stage again, you only need to cleanup/restore the target on that host and then run the target again.

Kill all the Java processes other than Node Manager. (Killing of the processes for Node Manager must be done twice.) Then run cleanup/restore:

```
./runProvisioning.sh -responseFile ./file_name.rsp -override
./overrides.properties -target cleanup-configure
```

```
./runProvisioning.sh -responseFile ./file_name.rsp -override
./overrides.properties -target restore-configure
```

Once the cleanup and restore builds are successful, you can run the configure target again.

This applies to all tasks related to configuring components.

Note: If the relative path for the response file (`./file_name.rsp`) and override properties (`./override.properties`) does not work, give a fully qualified path instead.

Task 1 Run the pre-configure phase

Before running the pre-configure phase, copy the `ORACLE_BASE/products/webtier_dmz_artifacts.zip` file from the `FINHOST1` non-DMZ computers to `WEBHOST1 ORACLE_BASE/products`.

Run the following commands from `ORACLE_BASE/repository/provisioning/bin`:

- **On `FINHOST1`:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target preconfigure`
- **On `WEBHOST1`:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target preconfigure`

Note: If pre-configure fails on `WEBHOST1` with Oracle Identity Manager split domain in an enterprise deployment environment, do the following:

1. On `WEBHOST1`, change directory to `ORACLE_BASE/config/phasesguards/preconfigure`.
 2. Delete the `WEBHOST1-FAILED.grd` file:
touch the file : `preconfigure-WEBHOST1-COMPLETED.grd`
-

Task 2 Run the configure phase

Run the following commands from `ORACLE_BASE/repository/provisioning/bin`:

- **On `FINHOST1`:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target configure`
- **On `WEBHOST1`:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target configure`

Task 3 Run the configure secondary phase

Run the following commands from *ORACLE_BASE/repository/provisioning/bin*:

- **On *FINHOST1*:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target configure-secondary`
- **On *WEBHOST1*:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target configure-secondary`

Task 4 Run the post-configure phase

Run the following commands from *ORACLE_BASE/repository/provisioning/bin*:

- **On *FINHOST1*:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target postconfigure`

Notes: For Oracle Identity Manager setup in single domain mode, do the following:

- Set this variable before running the post-configure stage:

```
$ export ORACLE_BI_HTTP_FMW_SHORT_TIMEOUT=120
```

- Change the value in the `wlst.sh` file located at *ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin*:

```
JVM_ARGS="-Dprod.props.file='${WL_HOME}'/.product.properties  
${WLST_PROPERTIES} ${JVM_D64} ${MEM_ARGS} ${CONFIG_JVM_ARGS}  
-Xms1024m  
-Xmx1024m"
```

- **On *WEBHOST1*:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target postconfigure`

Task 5 Run the start-up phase

Run the following commands from *ORACLE_BASE/repository/provisioning/bin*:

- **On *FINHOST1*:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target startup`
- **On *WEBHOST1*:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target startup`

Task 6 Run the validate phase

Run the following commands from *ORACLE_BASE/repository/provisioning/bin*:

- **On *FINHOST1*:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target validate`

Note: If validation is failing on *FINHOST1* with Oracle Identity Manager split domain with DMZ in an enterprise deployment environment, be aware that is an intermittent error. Repeat the process until the validation passes.

Note: If URLs are not redirecting to the Oracle Access Manager log in for Oracle Identity Manager split domain with DMZ in an enterprise deployment environment, restart the Oracle Access Manager server and the Administration Server to resolve the issue.

Note: If validation is failing with the message "Missing Entry config.xml" in a single domain Oracle Identity Manager setup in an enterprise deployment environment, comment out these lines in `ORACLE_BASE/repository/provisioning/provisioning-build/common-validate-build.xml`:

```
.
<if>
<istrue value="${ldap.server.type.valid}" />
<then>
<if>
<istrue value="${default.ldap.port.inuse}" />
<then>
<validateFileContains
filePath="${${component.key}.home.domain}/${${component.key}.domain
.name}/conf
ig/config.xml" >
<token value="${ldap.authenticator.type}" />
<token value="OAMIdentityAsserter" />
<token
value="${provisioning.include.idm.ldap.host.name}" />
</validateFileContains>
</then>
<else>
<validateFileContains
filePath="${${component.key}.home.domain}/${${component.key}.domain
.name}/conf
ig/config.xml" >
<token value="${ldap.authenticator.type}" />
<token value="OAMIdentityAsserter" />
<token
value="${provisioning.include.idm.ldap.host.name}" />
<token value="${ldap.port.tocheck}" />
</validateFileContains>
</else>
</if>
</then>
</if>
<logStatus state="BUILD_COMPLETE" category="security"
task="validateFileContains" />
```

- **On WEBHOST1:** `./runProvisioning.sh -responseFile ./file_name.rsp -override ./overrides.properties -target validate`

Note: Ignore any DMZ web-page-status validation failures.

Once all the scripts have run successfully, Oracle Fusion Financials provisioning is complete. For information about the resulting directory structure, see [Section 3.4.1, "Directory Structure."](#)

For information about the tasks these scripts perform, see *Oracle Fusion Applications Installation Guide*.

Task 7 Configure email servers

To configure an email server as a delivery channel to be used with Oracle Business Intelligence Publisher, see "Adding an E-mail Server" in the chapter "Setting Up Delivery Destinations" in *Oracle Fusion Middleware Administrator's Guide for Oracle Business Intelligence Publisher (Oracle Fusion Applications Edition)*.

5.5 Performing Post-Provisioning Tasks

After provisioning, there are several tasks you must perform.

5.5.1 Validation

After provisioning, access the following URLs, ensuring that the Administration console is visible:

- `http://fininternal.mycompany.com:7777/console`
- `http://crminternal.mycompany.com:7777/console`
- `http://hcminternal.mycompany.com:7777/console`
- `http://scminternal.mycompany.com:7777/console`
- `http://commoninternal.mycompany.com:7777/console`
- `http://biinternal.mycompany.com:7777/console`
- `http://prjinternal.mycompany.com:7777/console`
- `http://prcinternal.mycompany.com:7777/console`

For the following URLs, ensure that the Oracle Fusion Applications login screen is visible.

- `https://finexternal.mycompany.com/ledger/faces/LedgerWorkArea`
- `https://finexternal.mycompany.com/payables/faces/PaymentLandingPage`
- `https://prcexternal.mycompany.com/procurement/faces/PrcPoPurchasingWorkarea`
- `https://prjexternal.mycompany.com/projectsFinancials/faces/PRJProjectWorkarea`
- `https://commonexternal.mycompany.com/homePage/faces/AtkHomePageWelcome`
- `https://biexternal.mycompany.com/analytics`

5.5.2 Other Tasks

Other post-installation tasks include the following:

- Applying patches to your new environment
- Creating upgradeLDAPUsersForSSO.props
- Adding privileges to IDStore and Policy Store entities

- Reconciling users and roles from the IDStore into Oracle Identity Manager
- Deleting Oracle Business Intelligence restart files

For information about performing these tasks, see "Postinstallation Tasks" in *Oracle Fusion Applications Installation Guide*.

Scaling Out Oracle HTTP Server

The first Oracle HTTP Server was configured during the provisioning process (see [Chapter 5](#)). This chapter describes how to scale out Oracle HTTP Server for additional hosts.

This chapter includes the following topics:

- [Section 6.1, "Performing the Scaleout"](#)
- [Section 6.2, "Performing WebGate Post-Installation Steps"](#)
- [Section 6.3, "Installing WebGate Patches"](#)
- [Section 6.4, "Wiring Oracle HTTP Server with Load Balancer"](#)
- [Section 6.5, "Validating Oracle HTTP Server on WEBHOST2"](#)

6.1 Performing the Scaleout

To scale out Oracle HTTP Server:

1. Reboot *WEBHOST2* to start the scaleout from a clean machine.

Note: *WEBHOST2* and *WEBHOST1* should be identical machines.

2. Create the directory *ORACLE_BASE/repository/installers* with the same user that installed Oracle HTTP Server on *WEBHOST1*.

3. Copy or ftp the installers from *WEBHOST1* to *WEBHOST2*:

```
WEBHOST1> ORACLE_BASE/repository/installers/webgate
```

to

```
WEBHOST2> ORACLE_BASE/repository/installers
```

```
WEBHOST1> ORACLE_BASE/repository/installers/webtier
```

to

```
WEBHOST2> ORACLE_BASE/repository/installers
```

4. Run the following command to install Oracle Web Tier on *WEBHOST2* (oraInventory should be located in *ORACLE_BASE/oraInventory*):

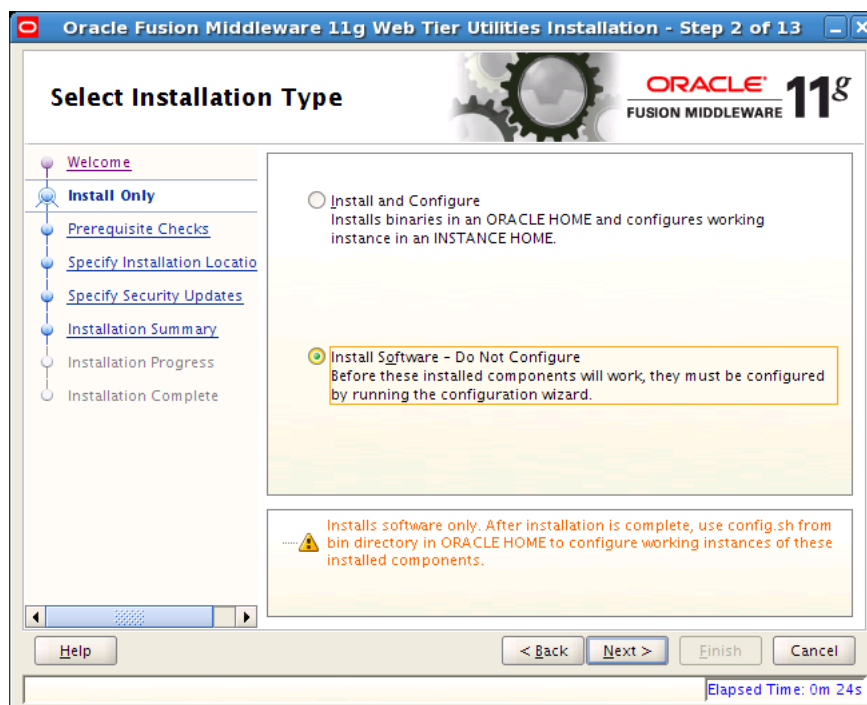
```
ORACLE_BASE/repository/installers/webtier/Disk1/runInstaller
```

The Oracle Fusion Middleware 11g Oracle Web Tier Utilities Configuration Welcome window opens.

5. Click **Next** to start the installation.

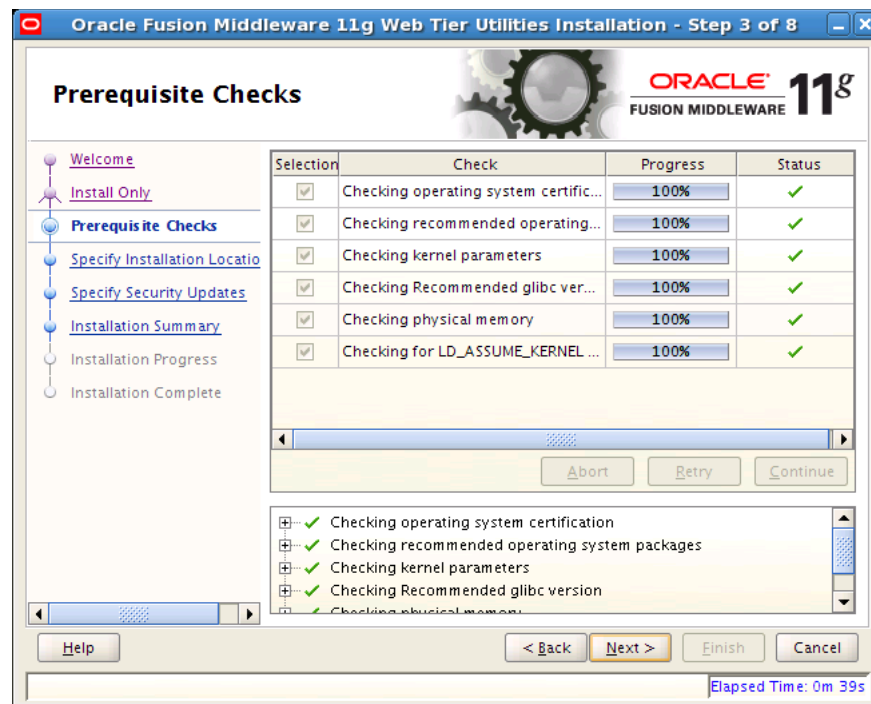
The Select Installation Type window, shown in [Figure 6-1](#), opens.

Figure 6-1 Select Installation Type Window

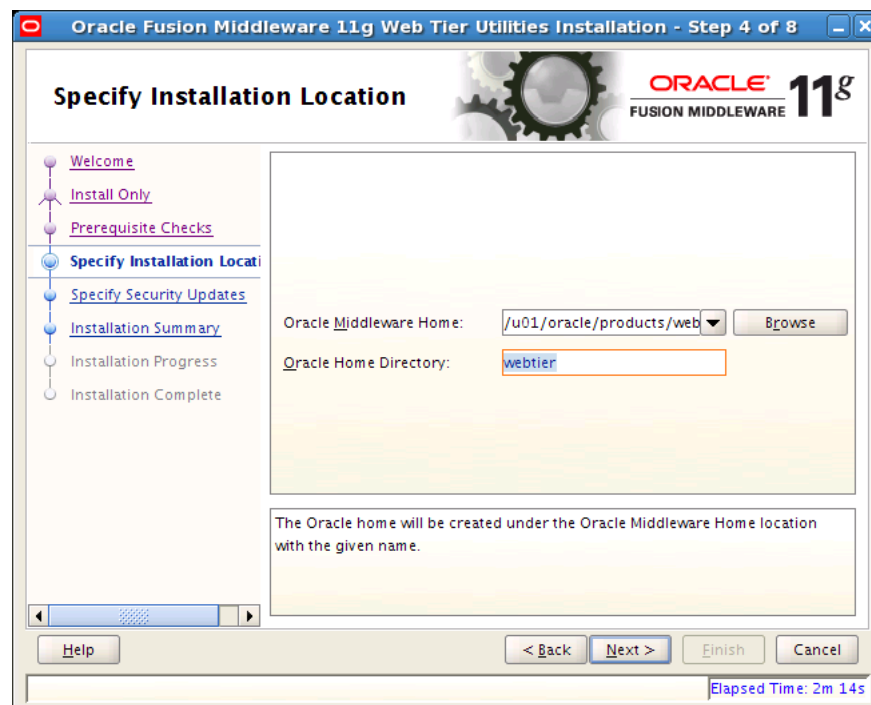


6. Select **Install Software - Do Not Configure** and click **Next**.

The Prerequisite Checks window, shown in [Figure 6-2](#), opens.

Figure 6–2 Prerequisite Checks Window

Click **Next**. The Specify Installation Location window, shown in Figure 6–3, opens.

Figure 6–3 Specify Installation Location Window

Select the path to Oracle Middleware Home and enter a name for the home directory. For example, /u01/oracle/products/webtier_mwhome/. Click **Next**.

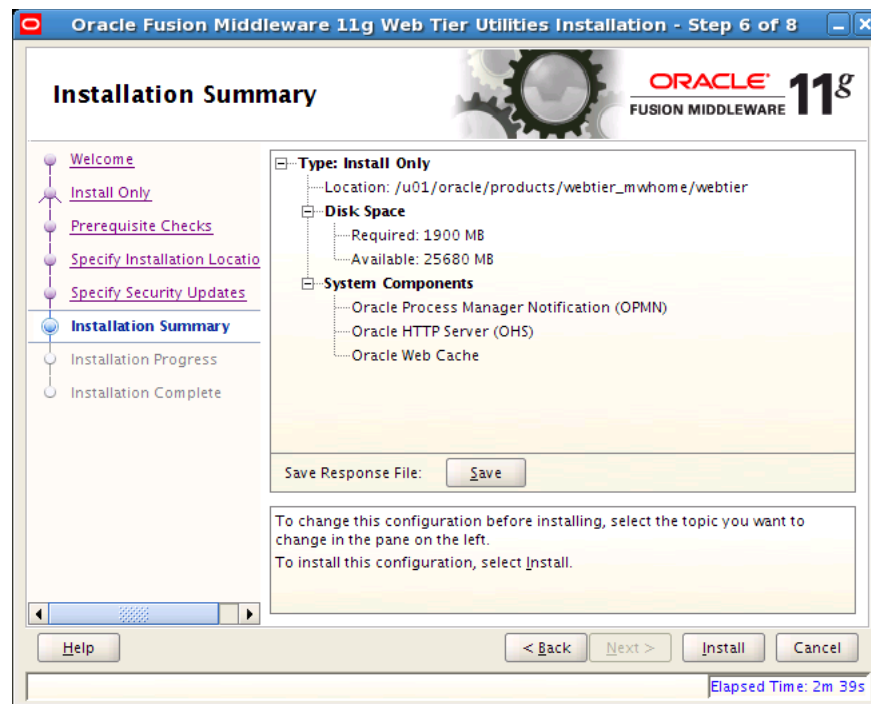
7. In the Specify Security Updates window, shown in Figure 6–4, do the following:

- Enter an email address
- Indicate that you wish to receive security updates from My Oracle Support
- Enter your My Oracle Support password

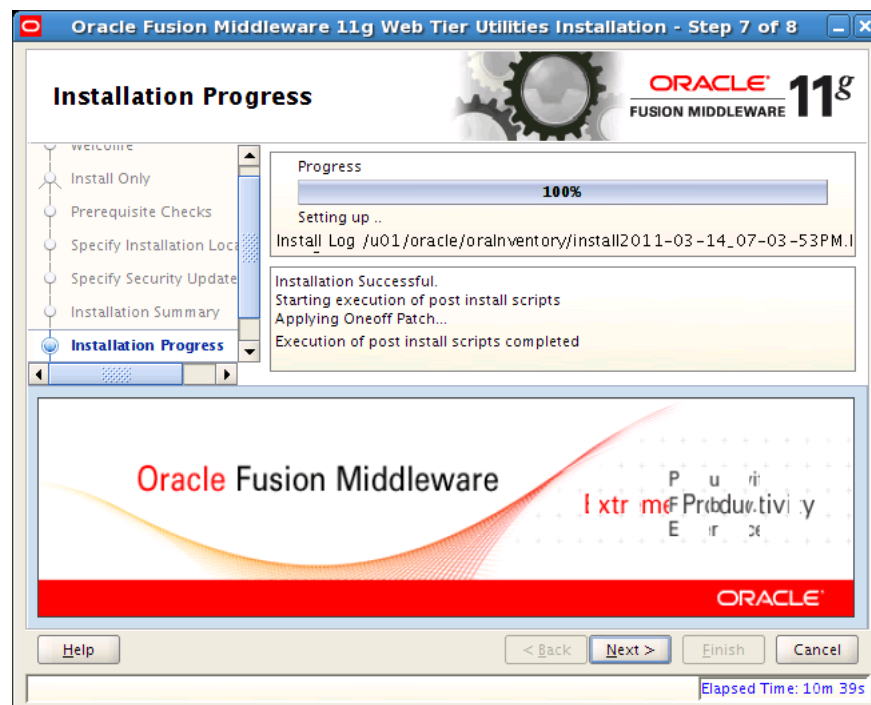
Figure 6–4 Specify Security Updates Window

The screenshot shows the 'Specify Security Updates' window during the Oracle Fusion Middleware 11g Web Tier Utilities installation. The window title is 'Oracle Fusion Middleware 11g Web Tier Utilities Installation - Step 5 of 8'. The Oracle logo and '11g' are in the top right. A left-hand navigation pane lists the installation steps: Welcome, Install Only, Prerequisite Checks, Specify Installation Location, Specify Security Updates (highlighted), Installation Summary, Installation Progress, and Installation Complete. The main content area has a heading 'Specify Security Updates' and a sub-heading 'Provide your email address to be informed of security issues, install the product and initiate configuration manager. [View details.](#)'. Below this, there is an 'Email:' label followed by a text input field. A note states: 'Easier for you if you use your My Oracle Support email address/username.' There is a checked checkbox with the text 'I wish to receive security updates via My Oracle Support.' and a 'My Oracle Support Password:' label followed by a password input field. At the bottom, there is a 'Help' button, '< Back' and 'Next >' buttons, and 'Finish' and 'Cancel' buttons. An 'Elapsed Time: 2m 24s' indicator is in the bottom right corner.

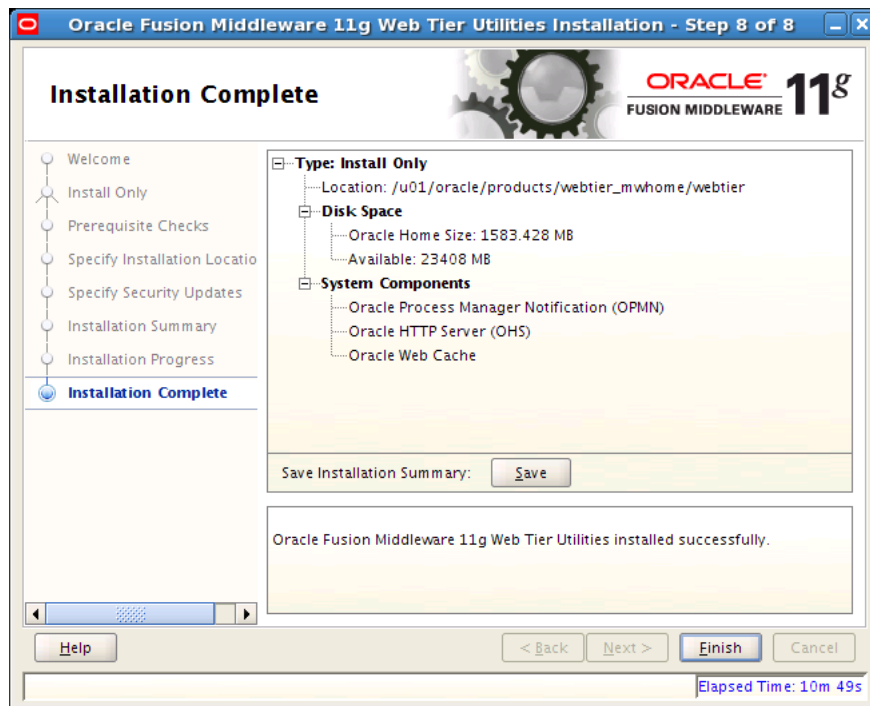
Click **Next**. The Installation Summary window, shown in [Figure 6–5](#), opens.

Figure 6–5 Installation Summary Window

8. Click **Install**. The Installation Progress window, shown in Figure 6–6, opens.

Figure 6–6 Installation Progress Window

Click **Next** when the installation has finished. The Installation Complete window, shown in Figure 6–7, opens.

Figure 6–7 Installation Complete Window

Click **Finish**.

9. View the directory structure that has been created:

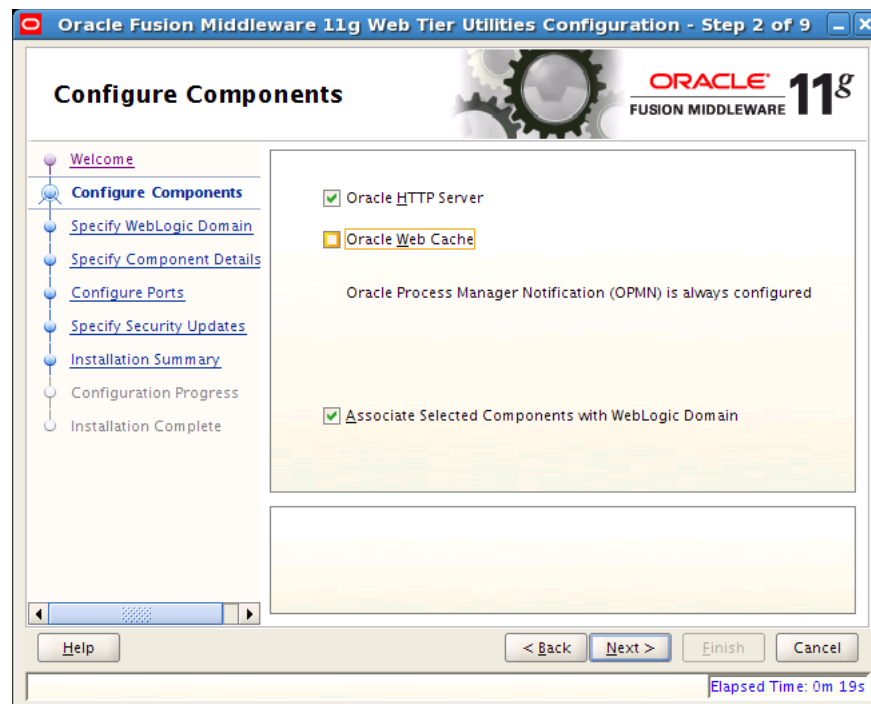
```
cd ORACLE_BASE/products/webtier_mwhome
```

10. Begin configuring the Oracle Web Tier components:

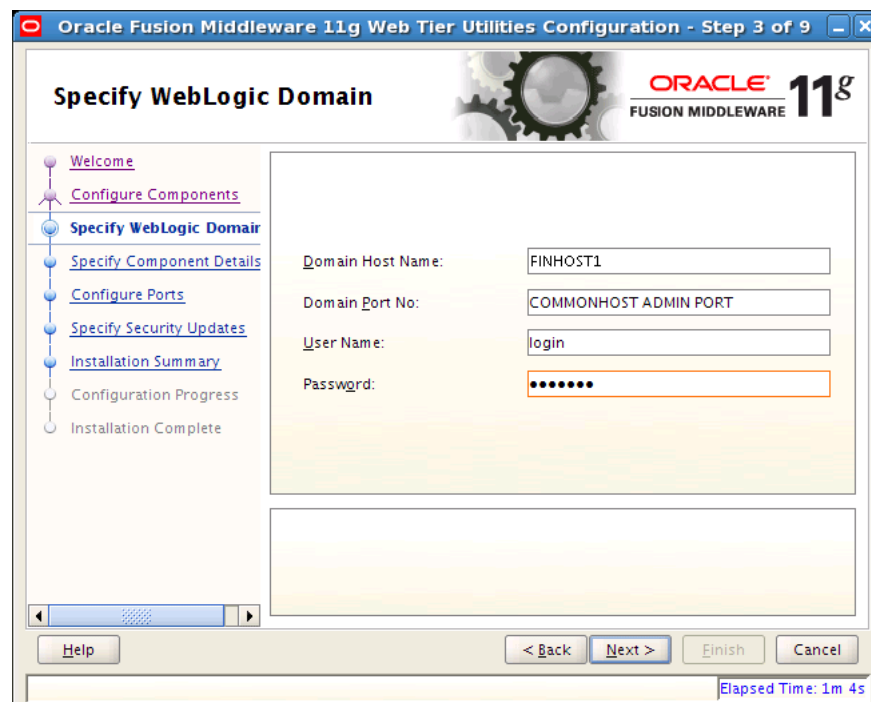
```
cd ORACLE_BASE/products/webtier_mwhome/webtier/bin
```

```
run ./config.sh
```

The Configure Components window, shown in [Figure 6–8](#), opens.

Figure 6–8 Configure Components Window

11. Select **Oracle HTTP Server** and **Associate Selected Components with WebLogic Domain**.
12. Click **Next**. The **Specify WebLogic Domain** window, shown in [Figure 6–9](#), opens.

Figure 6–9 Specify WebLogic Domain Window

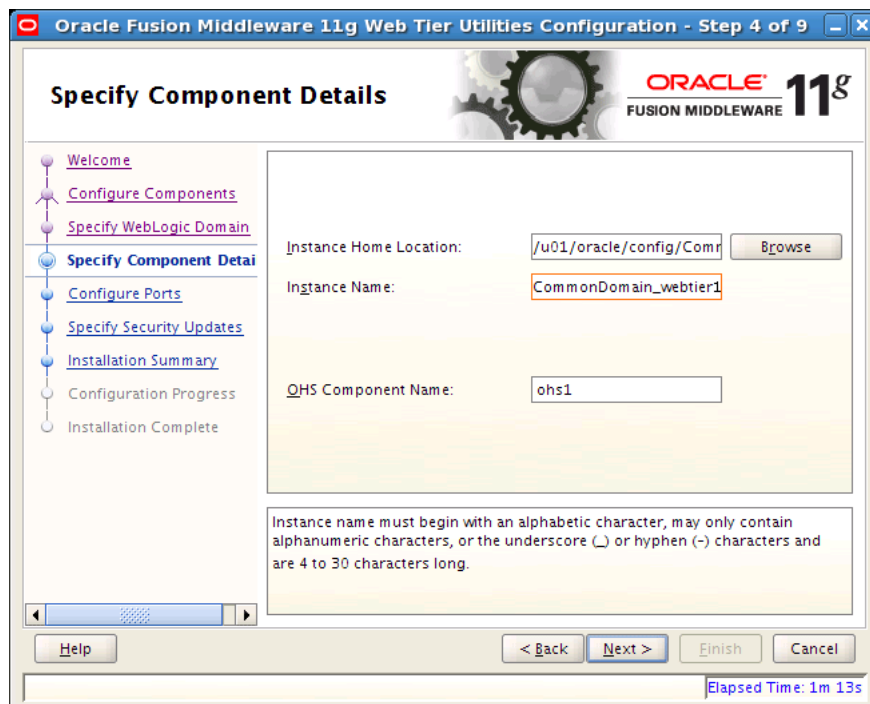
13. Enter the following:

- a domain host name; for example, FINHOST1
- a domain port number; for example, COMMONHOST ADMIN PORT
- your CommonDomain Administration Server user name
- your CommonDomainAdministration Server password

Note: Associate Oracle HTTP Server with the CommonDomain that Provisioning installed in [Chapter 5](#).

14. Click **Next**. The Specify Component Details window, shown in [Figure 6–10](#), opens.

Figure 6–10 Specify Component Details Window

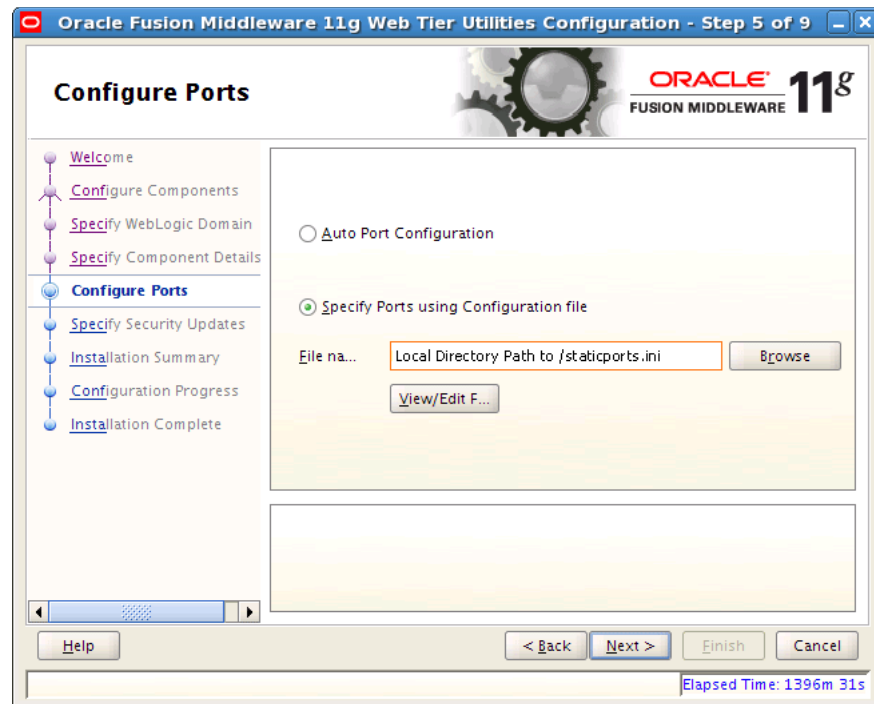


15. Do the following:

- Select the instance home location; for example, /u01/oracle/config/CommonDomain_webtier1
- Enter the instance name; for example, CommonDomain_webtier1
- Enter the Oracle HTTP Server component name; for example ohs1

16. Click **Next**. The Configure Ports window, shown in [Figure 6–11](#), opens.

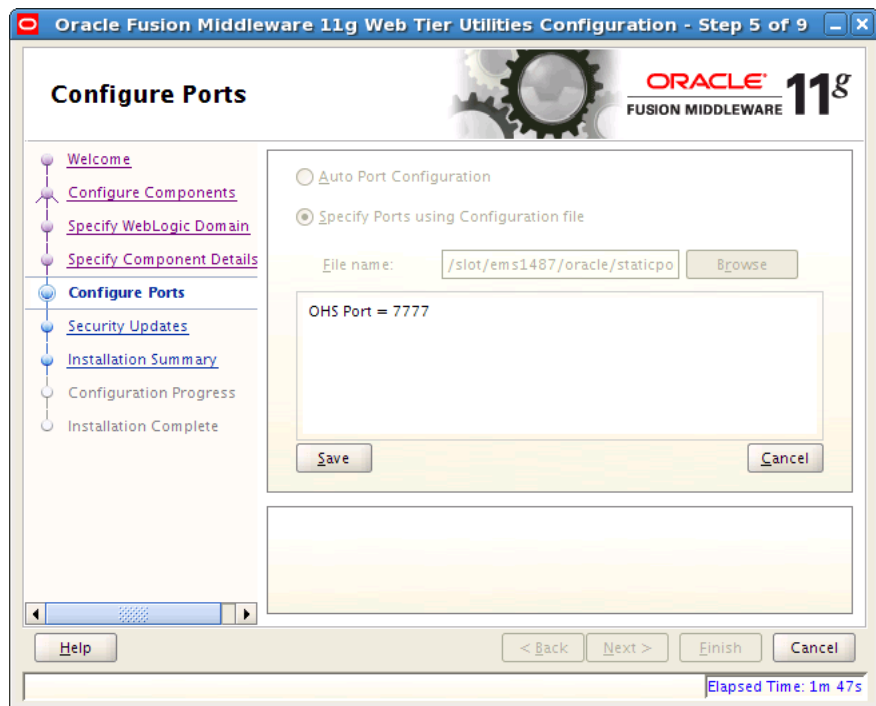
Figure 6–11 Configure Ports Window (1)



17. Select Specify Ports using Configuration file and click View/Edit.

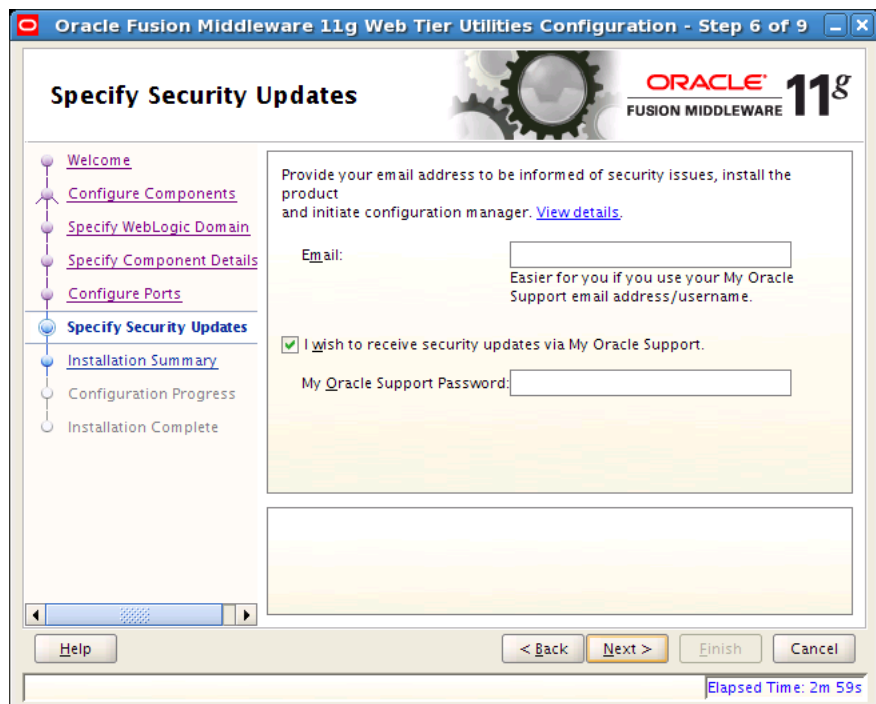
In the text field that displays, shown in Figure 6–12, enter OHS port = 7777.

Note: Copy the staticports.ini file from repository/installers/webtier/Disk1/stage/Response to ORACLE_BASE/staticports.ini.

Figure 6–12 Configure Ports Window (2)

Click **Save** and then click **Next**.

The Specify Security Updates window, shown in Figure 6–13, opens.

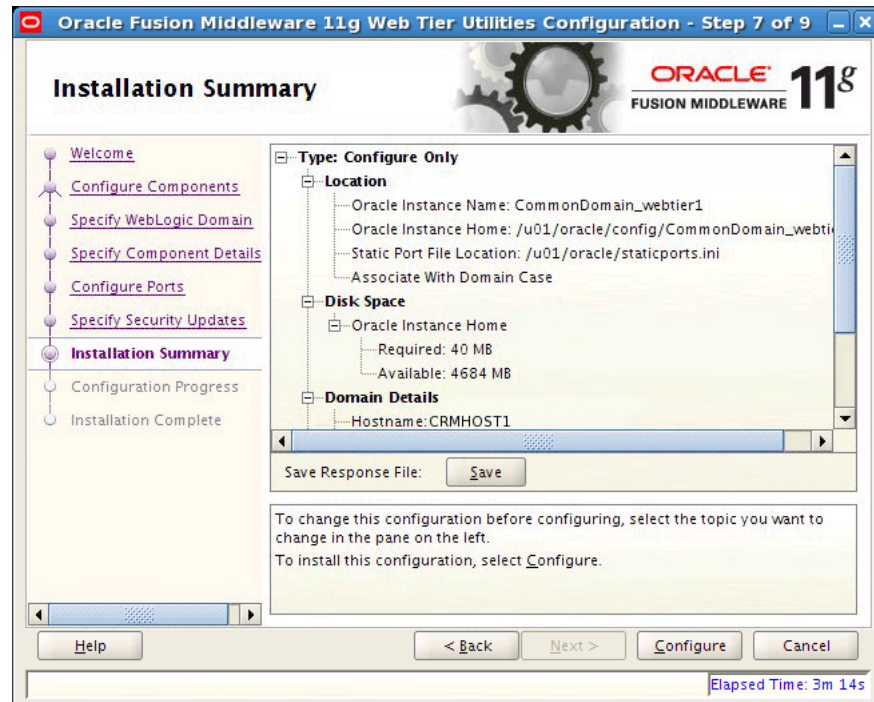
Figure 6–13 Specify Security Updates

18. Do the following:

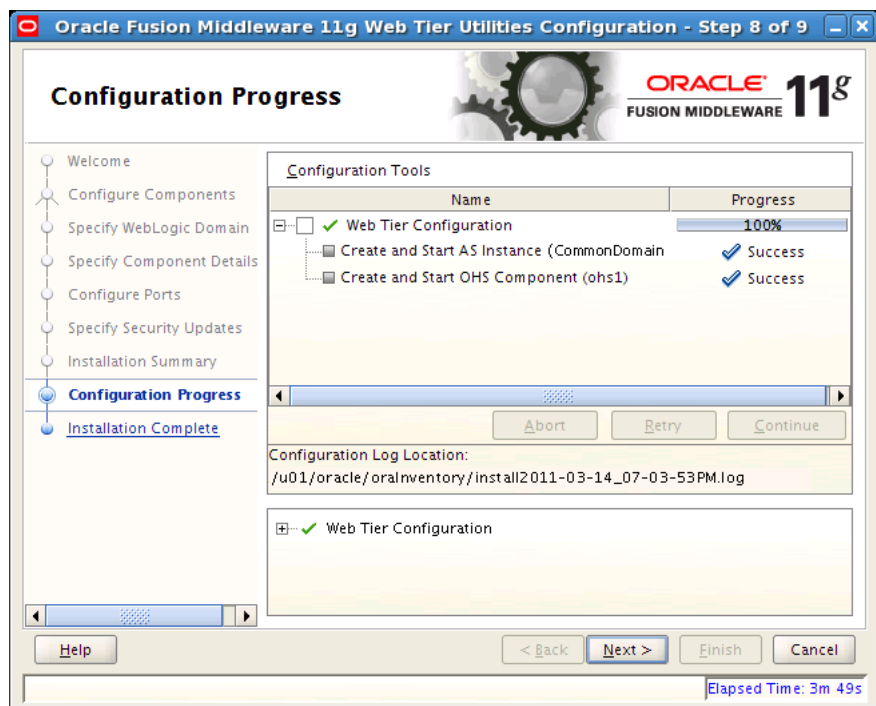
- Enter an email address

- Indicate that you wish to receive security updates from My Oracle Support
 - Enter your My Oracle Support password
19. Click **Next**. The Installation Summary window, shown in Figure 6–14, opens.

Figure 6–14 Installation Summary Window

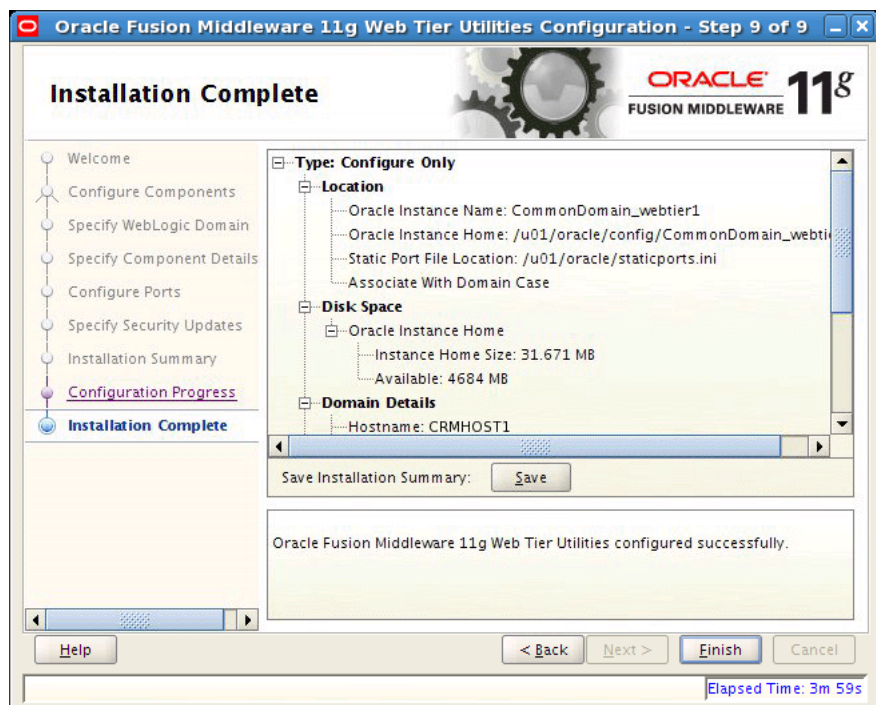


20. Click **Configure** to install the configuration. The Configuration Progress window, shown in Figure 6–15, opens.

Figure 6–15 Configuration Progress Window

21. Click **Next**.

When the installation completes, the Installation Complete window, shown in [Figure 6–16](#), opens.

Figure 6–16 Installation Complete Window

22. Click **Finish**.

23. Copy or ftp the FusionVirtualHost files from *WEBHOST1* to *WEBHOST2*:

```
WEBHOST1> ORACLE_BASE/config/CommonDomain_webtier/config/OHS/ohs1/moduleconf
```

to

```
WEBHOST2> ORACLE_BASE/config/CommonDomain_webtier1/config/OHS/ohs1/moduleconf/
```

24. After the copy, change all *WEBHOST1* entries in the *.conf* files to *WEBHOST2*.

25. Restart the Oracle HTTP Server instance:

```
WEBHOST2> cd ORACLE_BASE/config/CommonDomain_webtier1/bin
```

```
WEBHOST2> ./opmnctl stopall
```

```
WEBHOST2> ./opmnctl startall
```

26. From *ORACLE_BASE/repository/installers/webgate/Disk1*, start the WebGate installation:

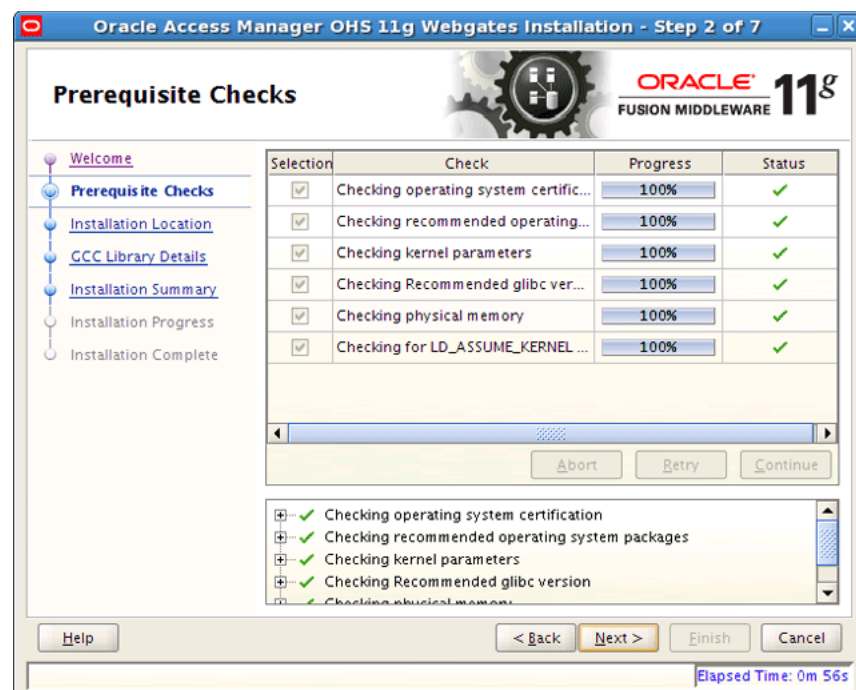
```
./runInstaller
```

27. When prompted, specify the path to the JDK:

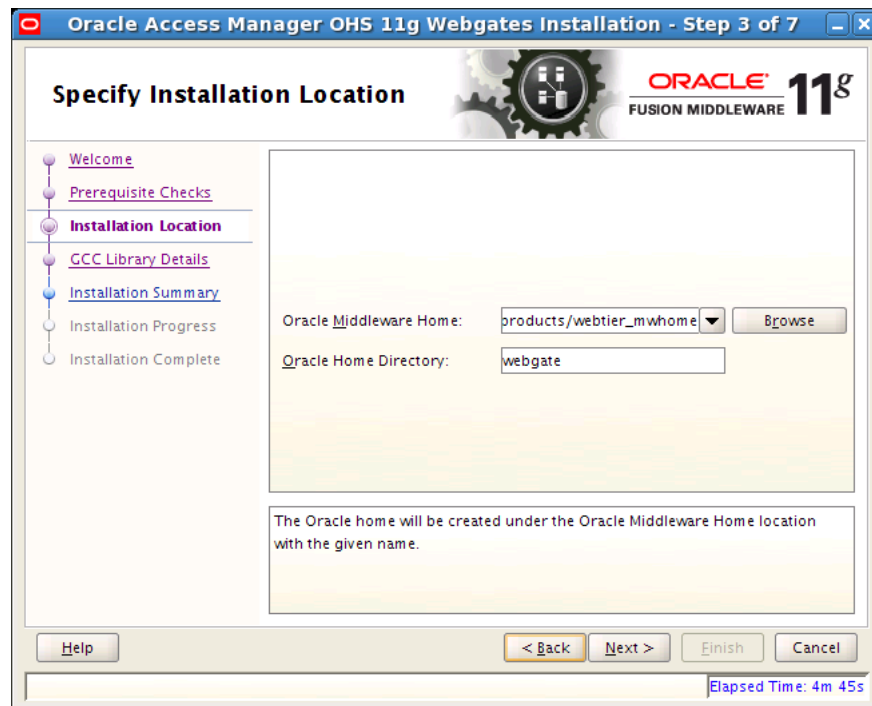
```
ORACLE_BASE/repository/jdk6
```

28. When the Welcome window opens, click **Next**. The Prerequisite Checks window, shown in [Figure 6-17](#), opens.

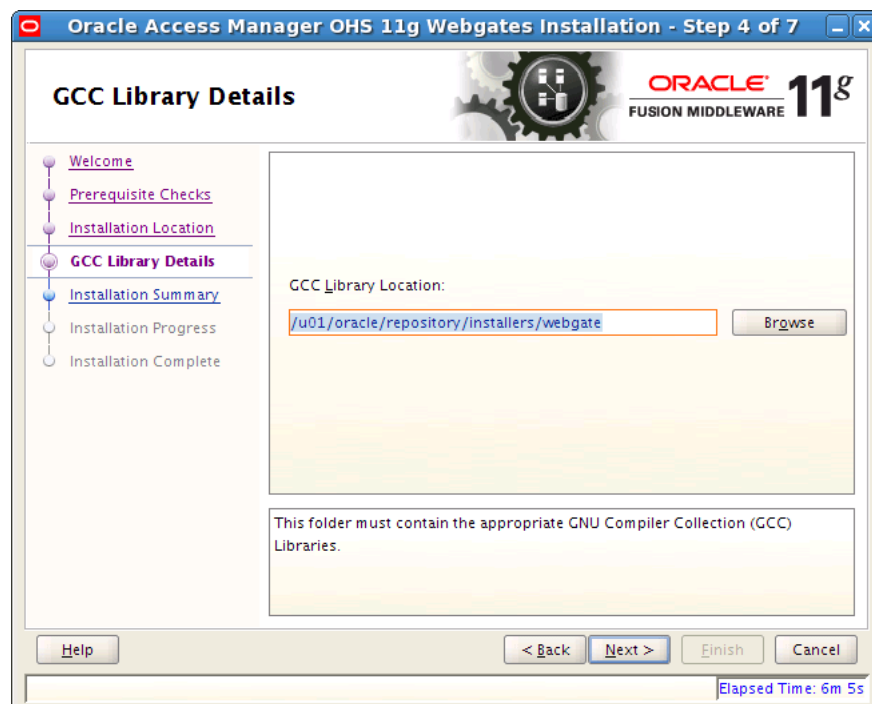
Figure 6-17 Prerequisite Checks Window



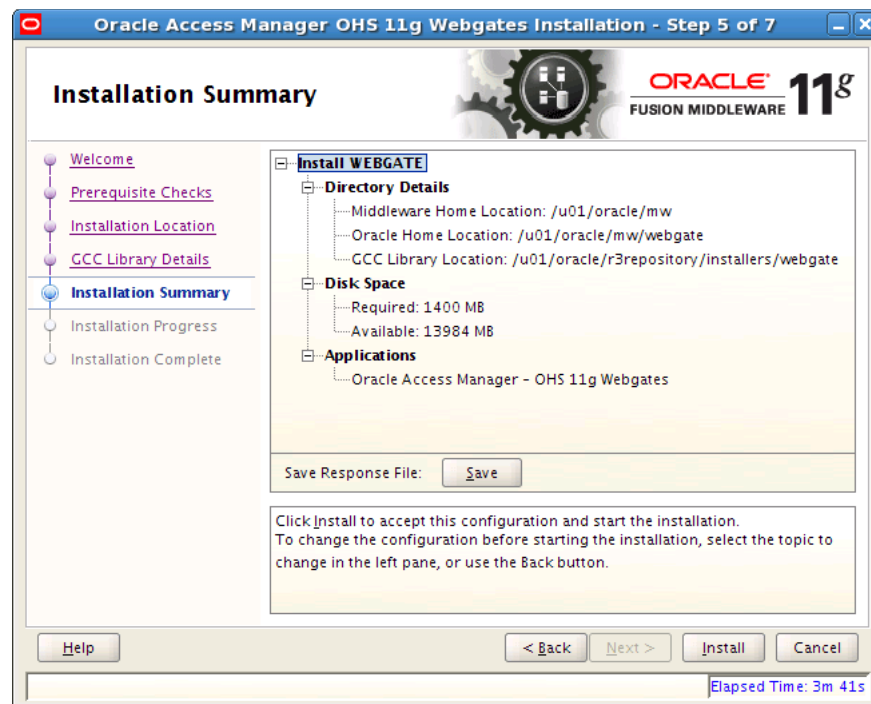
29. When the checking process completes, click **Next**. The Installation Location window, shown in [Figure 6-18](#), opens.

Figure 6–18 Installation Location Window

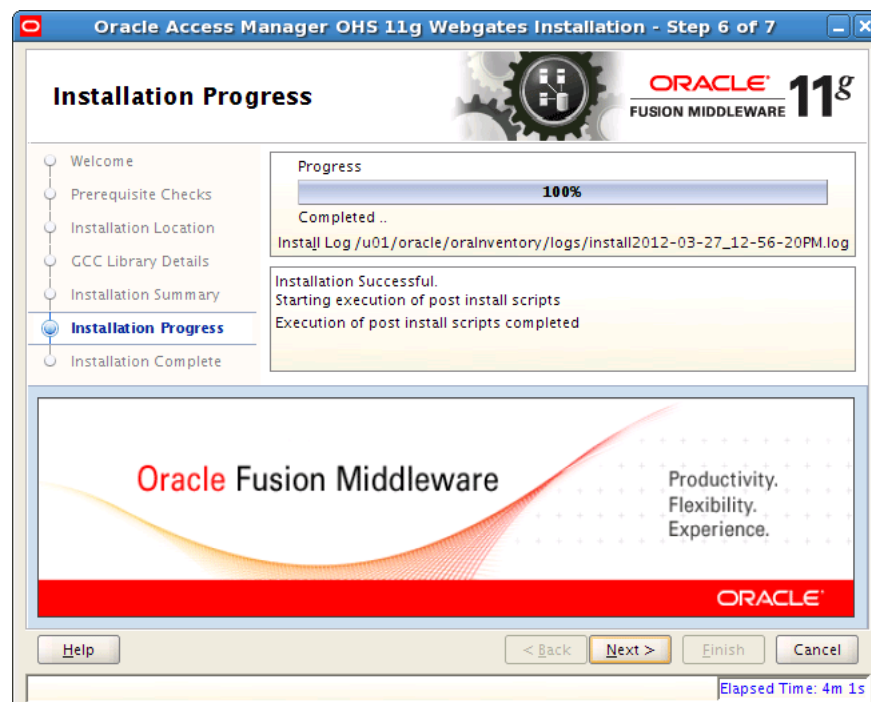
30. Enter an Oracle Middleware Home location Oracle Home Directory and click **Next**. The GCC Library Details window, shown in [Figure 6–19](#), opens.

Figure 6–19 GCC Library Details Window

31. Enter the location for the GCC runtime libraries and click **Next**. The Installation Summary window, shown in [Figure 6–20](#), opens.

Figure 6–20 Installation Summary Window

32. Click **Save** if you wish to save the response file. Click **Install** to start the installation. Following an interim window, the one shown in Figure 6–21 opens. During installation, a progress window, shown in Figure 6–21, opens.

Figure 6–21 Installation Progress Window

33. When the installation finishes, click **Next**. The Installation Complete window opens.
34. Click **Save** if you wish to save the installation details. Click **Finish** to complete the WebGate installation.

6.2 Performing WebGate Post-Installation Steps

After installing WebGate, do the following:

1. Add `LD_LIBRARY_PATH` to `ORACLE_BASE/products/webtier_mwhome/webtier/lib`.
2. Run the following commands:

```
# Usage: deployWebGateInstance.sh -w <WebGate_instancedir> -oh WebGate_Oracle_Home
```

```
$ cd ORACLE_BASE/products/webtier_mwhome/webgate/webgate/ohs/tools/
deployWebGate
```

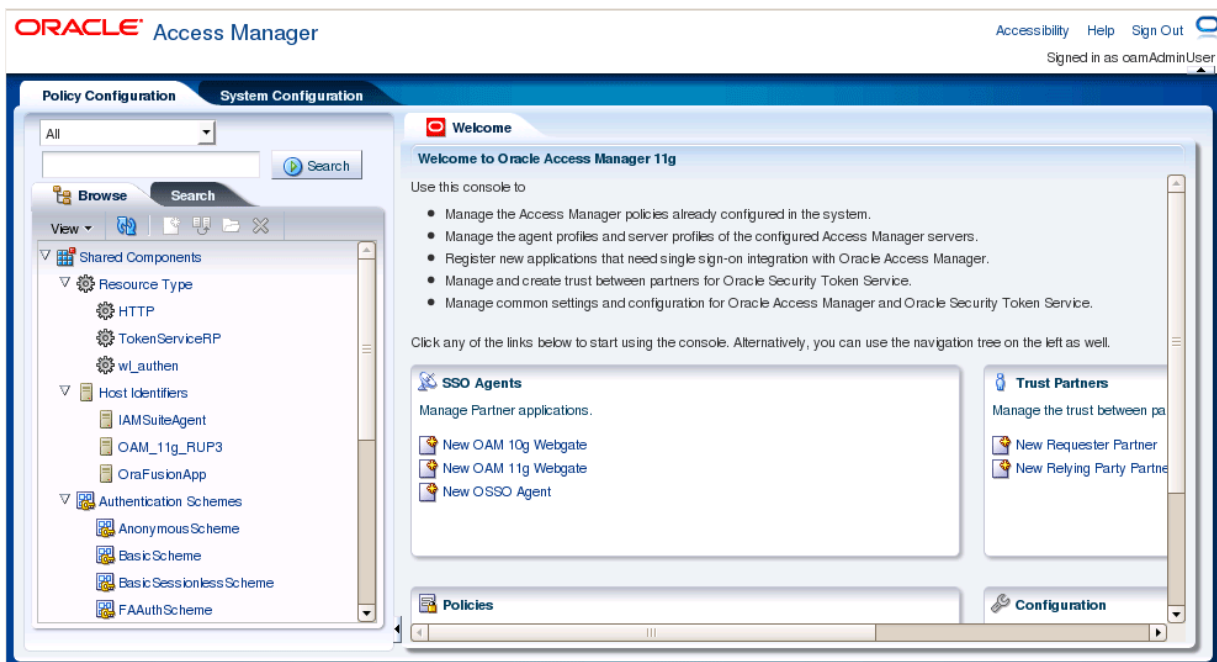
```
$ ./deployWebGateInstance.sh -w ORACLE_BASE/config/CommonDomain_
webtier1/config/OHS/ohs1 -oh ORACLE_BASE/products/webtier_mwhome/webgate
```

```
$ cd /ORACLE_BASE/products/webtier_mwhome/webgate/webgate/ohs/tools/setup/
InstallTools
```

```
$ ./EditHttpConf -w ORACLE_BASE/config/CommonDomain_webtier1/config/OHS/ohs1
-oh ORACLE_BASE/products/webtier_mwhome/webgate -o webgate.conf
```

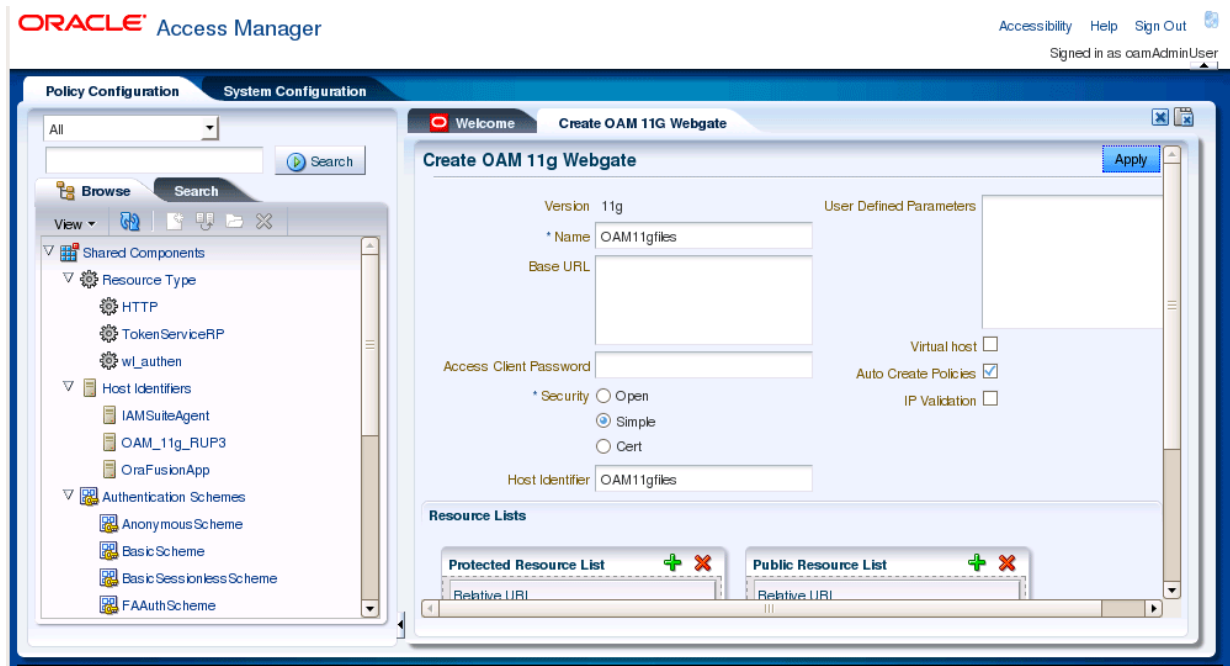
3. Log in to your Oracle Access Manager server.
4. In the list of SSO Agents, shown in [Figure 6-22](#), click "New OAM 11g Webgate".

Figure 6-22 Oracle Access Manager (1)



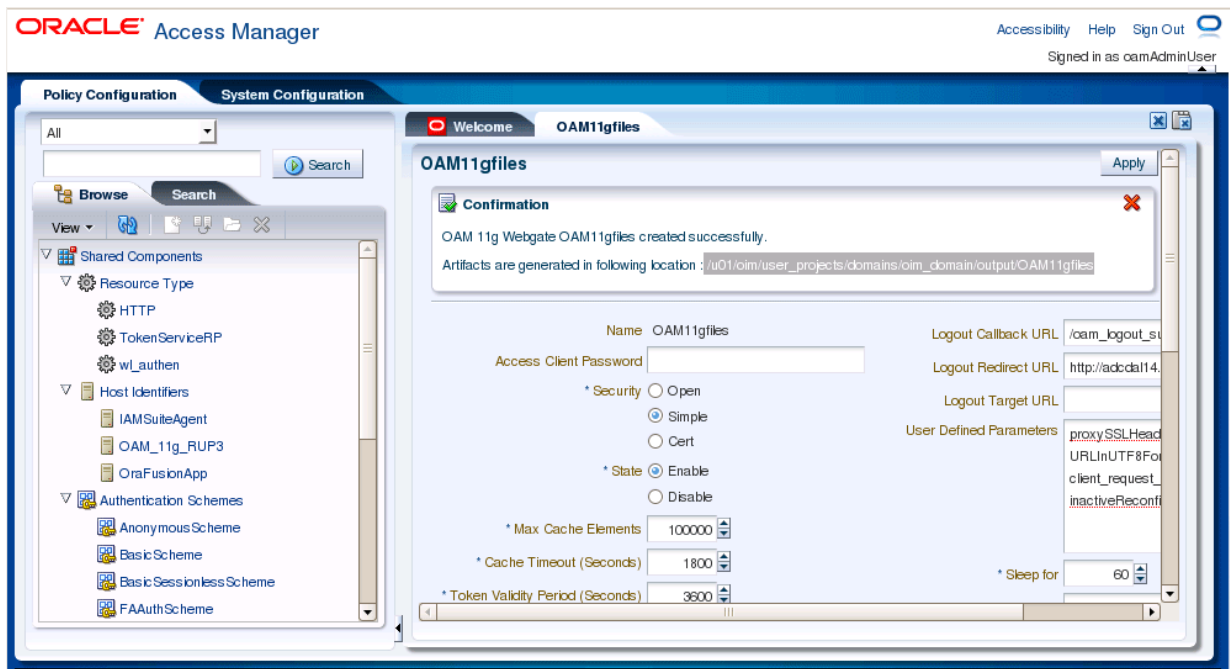
5. From the **Create OAM 11G Webgate** tab, shown in [Figure 6-23](#), enter a name and click **Apply**.

Figure 6–23 Oracle Access Manager (2)



- From the **OAM11gfilestab**, shown in Figure 6–23, note the location of where the artifacts are generated on the **IDMHOST** machine. These artifacts should be copied to **WEBHOST2**.

Figure 6–24 Oracle Access Manager (3)



- Copy the artifacts files from the **IDMHOST** machine to **ORACLE_BASE/config/CommonDomain_webtier1/config/OHS/ohs1/webgate/config** on **WEBHOST2**.

Run the following commands from *WEBHOST2*:

```
cd ORACLE_BASE/config/CommonDomain_webtier1/config/OHS/ohs1/webgate/config
$ cp FROM OAMHOST ( location_of_artifacts)/ObAccessClient.xml .
$ cp FROM OAMHOST ( location_of_artifacts)/cwallet.sso .
$ cp FROM OAMHOST ( location_of_artifacts)/password.xml .
$ cd simple
$ cp FROM OAMHOST ( location_of_artifacts)/aaa_key.pem .
$ cp FROM OAMHOST ( location_of_artifacts)/aaa_cert.pem .
```

6.3 Installing WebGate Patches

If the *ORACLE_BASE/repository/installers/webgate* location has a patch directory, perform the steps in this section. If prompted, specify the JDK location.

To install WebGate patches, do the following:

1. Change directory to *ORACLE_BASE/repository/installers/webgate/patch/*.
2. If the directory under patch exists, set the path to the *Opatch* directory to *ORACLE_BASE/products/webgate/OPatch*.

Note: Running the `$ which opatch` command will give you the path specified in Step 2.

3. Install all the patches in *ORACLE_BASE/repository/installers/webgate/patch/*.
4. Run the following command:

```
./opatch apply
```

After you install the patches, restart the web server. Oracle HTTP Server scaleout is complete, and *WEBHOST1* and *WEBHOST2* should behave identically.

6.4 Wiring Oracle HTTP Server with Load Balancer

Configure your load balancer to route all HTTP requests to the hosts running Oracle HTTP Server, that is, *WEBHOST1* and *WEBHOST2*.

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

You also must set Monitors for HTTP.

6.5 Validating Oracle HTTP Server on WEBHOST2

To validate once the installation is complete:

1. Check that it is possible to access the Oracle HTTP Server home page using the following URLs:
 - `http://webhost1.mycompany.com:10601`
 - `http://webhost2.mycompany.com:7777`
2. Stop *WEBHOST1*:

```
WEBHOST1> cd /u01/oracle/config/CommonDomain_webtier/bin
```

```
WEBHOST1> ./opmnctl stopall
```

3. Access the following URLs to ensure that the Administration console is visible:

- <http://fininternal.mycompany.com:7777/console>
- <http://hcminternal.mycompany.com:7777/console>
- <http://scmininternal.mycompany.com:7777/console>
- <http://commoninternal.mycompany.com:7777/console>
- <http://biinternal.mycompany.com:7777/console>
- <http://prjinternal.mycompany.com:7777/console>
- <http://prcinternal.mycompany.com:7777/console>

4. Access the following URLs to ensure that the Oracle Fusion Applications login screen is visible:

- <https://finexternal.mycompany.com/ledger/faces/LedgerWorkArea>
- <https://finexternal.mycompany.com/payables/faces/PaymentLandingPage>
- <https://prcexternal.mycompany.com/procurement/faces/PrcPoPurchasingWorkarea>
- <https://prjexternal.mycompany.com/projectsFinancials/faces/PRJProjectWorkarea>
- <https://commonexternal.mycompany.com/homePage/faces/AtkHomePageWelcome>
- <https://biexternal.mycompany.com/analytics>

5. Run the following commands:

```
WEBHOST1> cd /u01/oracle/config/CommonDomain_webtier/bin
```

```
WEBHOST1> ./opmnctl startall
```

Setting Up Node Manager for an Enterprise Deployment

This chapter describes how to configure Node Manager in accordance with enterprise deployment recommendations.

This chapter includes the following topics:

- [Section 7.1, "Setting Up Node Manager for FINHOST2"](#)
- [Section 7.2, "Creating the Identity Keystore on FINHOST2"](#)

7.1 Setting Up Node Manager for FINHOST2

Do the following:

1. Run the following command:

```
FINHOST2> cd ORACLE_BASE/products/fusionapps/wlserver_10.3/common/nodemanager
```

2. In the `nodemanager` directory, copy the content of the node-specific directory to *FINHOST2*. In this case, *FINHOST1* is the node-specific directory.

```
FINHOST2> cp -r FINHOST1 FINHOST2
```

3. Change directory to *FINHOST2*. You should see the following files:

```
nm_data.properties  nodemanager.log  startNodeManagerWrapper.sh
nodemanager.domains  nodemanager.properties
```

Note: Manually delete any lock files that may be present. For example, `nodemanager.log.lck`.

4. In the `nodemanager.domains` file, edit all the domain paths that are local to *FINHOST2*. For example,
`FINDomain=/u02/local/oracle/config/domains/FINHOST2/FINDomain.`

Note: Because `BIDomain` is a bit different, an example path would be
`BIDomain=/u02/local/oracle/config/domains/FINHOST1/BIDomain.`

5. In the `startNodeManagerWrapper.sh` file, change `NM_HOME` to `ORACLE_BASE/products/fusionapps/wlserver_10.3/common/nodemanager/FINHOST2`.
6. In the `nodemanager.properties` file:

- Add or modify the following lines:

```
KeyStores=CustomIdentityAndCustomTrust
CustomIdentityKeyStoreFileName=ORACLE_BASE/products/fusionapps/wlserver_
10.3/server/lib/FINHOST2_fusion_identity.jks
CustomIdentityPrivateKeyPassPhrase=keypassword
CustomIdentityAlias=FINHOST2_fusion
```

Note: *keypassword* is the password given in the *ORACLE_BASE/repository/provisioning/provisioning-plan/enterprise_devtxk_generic.properties* file

- Ensure that the path to the local machine */u02/local/oracle/nodemanager/* exists, and that the *LogFile* value is pointing to */u02/local/oracle/nodemanager/FINHOST2.log*.
- Ensure that the path for *DomainsFile* and *NodeManagerHome* are correct for *FINHOST2*.

7.2 Creating the Identity Keystore on FINHOST2

Provisioning has created the identity keystore *FINHOST1_fusion_identity.jks* for *FINHOST1*. Subsequently, the identity keystore *FINHOST2_fusion_identity.jks* must be created for *FINHOST2*.

Do the following to create the keystore:

1. Change directory to *ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib*.

Ensure the *FINHOST1_fusion_identity.jks* and *fusion_trust.jks* files are present.

2. Back up *fusion_trust.jks* to *fusion_trust.jks.org*.
3. Run the following command to set the CLASSPATH:

```
FINHOST2> source ORACLE_BASE/products/fusionapps/wlserver_10.3/server/
/bin/setWLSEnv.sh
```

Ensure that the CLASSPATH has been set:

```
FINHOST2> which keytool
```

The output should point to the *ORACLE_BASE/products/fusionapps/jdk6/jre/bin/keytool*.

4. Run the following command to create the keypair for *FINHOST2_fusion_identity.jks*:

```
FINHOST2> keytool -genkeypair -keyalg RSA -alias FINHOST2_fusion -keypass
keypassword -keystore FINHOST2_fusion_identity.jks -storepass keystorepassword
-validity 180 -dname 'CN=FINHOST2, OU=defaultOrganizationUnit,
O=defaultOrganization, C=US'
```

where

- *keystorepassword* is the password given in the provisioning response file (check *provisioning.setup.common.core.keystore.password* in the provisioning response file)

- *keypassword* is the password given in the provisioning response file (check `provisioning.setup.common.core.key.password` in the provisioning response file)

Notes:

- It is recommended to keep the commands in a file and then execute it.
 - Since the passwords in the response file are encrypted, take note of or save the passwords when you are creating the response file.
-

5. Run the following command to export the certs:

```
FINHOST2> keytool -exportcert -alias FINHOST2_fusion
-keystore FINHOST2_fusion_identity.jks
-storepass keystorepassword -rfc -file /tmp/appIdentityKeyStore.jks
```

Note: If the alias *FINHOST2_fusion* exists, run this command to delete it:

```
keytool -delete -alias FINHOST2_fusion -keystore fusion_trust.jks
-storepass keystorepassword
```

The following command will display the certificates in the trust keystore:

```
keytool -list -keystore fusion_trust.jks -storepass
keystorepassword
```

6. Run the following command to import the certs:

```
FINHOST2> keytool -importcert -noprompt -alias FINHOST2_fusion -file
/tmp/appIdentityKeyStore.jks -keystore fusion_trust.jks -storepass
keystorepassword
```

7. Verify that the file *FINHOST2_fusion_identity.jks* has been created in the directory *ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib* directory.
8. Start Node Manager on *FINHOST2* by running the following command:

```
ORACLE_BASE/products/fusionapps/wlserver_10.3/common/nodemanager/FINHOST2/
startNodeManagerWrapper.sh &
```

Scaling Out the Oracle Fusion Financials Domain

This chapter describes how to scale out the Oracle Fusion Financials domain.

This chapter includes the following topics:

- [Section 8.1, "Overview of the Oracle Fusion Financials Domain"](#)
- [Section 8.2, "Prerequisites for Scaling Out the Oracle Fusion Financials Domain"](#)
- [Section 8.3, "Adding a New Machine in the Oracle WebLogic Server Console"](#)
- [Section 8.4, "Packing and Unpacking the Managed Server Domain Home"](#)
- [Section 8.5, "Cloning Managed Servers and Assigning Them to FINHOST2"](#)
- [Section 8.6, "Oracle HTTP Server Configuration"](#)
- [Section 8.7, "Configuring Server Migration for the Managed Servers"](#)
- [Section 8.8, "Validating the System"](#)

8.1 Overview of the Oracle Fusion Financials Domain

The Oracle Fusion Financials domain provides Oracle Fusion Financials with Currency, Calendar, and other functionality. The Oracle Fusion Financials domain exposes setup portlets that the Oracle Fusion Financials implementation manager can use via Functional Setup Manager.

[Figure 2–3 in Chapter 2, "Introduction to the Enterprise Deployment Reference Topologies,"](#) shows the topology for the Oracle Fusion Financials domain within the overall reference enterprise deployment topology.

8.2 Prerequisites for Scaling Out the Oracle Fusion Financials Domain

Before you begin, ensure the following:

- Node Manager has been started in the Secure Sockets Layer (SSL) mode by following the instructions in [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"](#)
- You are starting with a clean machine if it is the first time it is being used for a scale out
- The `/etc/hosts` file has proper entries. To verify, ping this machine with the fully qualified name of the machine
- The user created on `FINHOST2` should be the same as the user on `FINHOST1`

- The directory structure `/u01/oracle` is mounted to same shared file system as *FINHOST1*
- The directory structure `/u02/local/oracle/config` on *FINHOST2* has been created
- The initial Oracle Fusion Financials deployment on *FINHOST1* has already been done and verified by provisioning

8.3 Adding a New Machine in the Oracle WebLogic Server Console

To add a new machine:

1. Log in to the Administration Server:
`http://fininternal.mycompany.com:7777/console.`
2. Navigate to **FinancialDomain > Environment > Machines.**
LocalMachine is located in the right-hand pane.
3. In the left-hand pane, click **Lock & Edit.**
4. In the right-hand pane, first click **New** to add the remote machine, and then specify the following:
 - Name - enter *FINHOST2*
 - Machine operating system - Unix
5. Click **Next.**
6. In the window that opens, set the following attributes:
 - Type - SSL
 - Listen Address - `<FINHOST2>`

Note: The "localhost" default value here is wrong.

- Listen port - 5556
7. Click **Finish** and activate the changes.

Note: If you get an error when activating the changes, see [Section 20.8.18, "Administration Console Redirects from Internal URL to Container URL after Activation"](#) for the temporary solution.

8.4 Packing and Unpacking the Managed Server Domain Home

Since the *FINHOST1* domain directory file system is also available from *FINHOST2*, both pack and unpack commands can be executed from *FINHOST2*.

To pack and unpack the Managed Server domain home:

1. Change directory to `ORACLE_BASE/products/fusionapps/oracle_common/common/bin.`
2. Run the pack command:

```
FINHOST2> ./pack.sh -managed=true -domain=ORACLE_BASE/config/domains/  
FINHOST1/FinancialDomain -template=ORACLE_BASE/user_templates/  
FinancialDomain_managed.jar -template_name=  
"Financial_Managed_Server_Domain"
```

3. Ensure that `/u02/local/oracle/config/domains/FINHOST2/FinancialDomain` is empty, and then run the unpack command:

```
FINHOST2> ./unpack.sh -domain=/u02/local/oracle/config/domains/FINHOST2/
FinancialDomain -template=ORACLE_BASE/user_templates/
FinancialDomain_managed.jar
```

Here, `ORACLE_BASE` is shared, and `/u02/local` is local to `FINHOST2`.

8.5 Cloning Managed Servers and Assigning Them to FINHOST2

To add a Managed Server and assign it to `FINHOST2`:

1. Log in to the Administration Server:
`http://fininternal.mycompany.com:7777/console.`
2. Navigate to **FinancialDomain > Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the *Managed_Servers* checkbox (for example, **GeneralLedgerServer_1**) and then click **Clone**.
5. Specify the following Server Identity attributes:

- Server Name - `GeneralLedgerServer_2`

Note: To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to "_2".

- Server Listen Address - `<FINHOST2>`
- Server Listen Port - leave "as is"

Note: For Oracle SOA Suite server, add a port value that is different than the `soa_server1` server value. This will help in server migration.

6. Click **OK**.

You now should see the newly cloned server, `GeneralLedgerServer_2`.

7. Click **GeneralLedgerServer_2** and change the following attributes:
 - Machine - `<FINHOST2>`
 - Cluster Name - accept the default, `GeneralLedgerCluster`

Note: Ensure that this cluster name is the same as the cluster name of the original Managed Server.

8. Click **Save** and then **Activate Changes**.
9. Navigate to **FinancialDomain > Environment > Servers**.
10. From the **Name** column, click the **GeneralLedgerServer_2** scaled-out server link.

11. Click **Lock & Edit**, and then select the **Configuration** tab.
12. Select the **Keystores** tab, and ensure that the keystores value is **Custom Identity and Custom Trust**.
13. Do the following:
 - a. Change the Custom Identity Keystore path to point to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/FINHOST2_fusion_identity.jks` file.
 - b. Leave the Custom Identity Keystore type blank.
 - c. Change the Custom Identity Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
 - d. Re-enter the Confirm Custom Identity Keystore Passphrase.
 - e. Ensure that the Confirm Custom Trust Keystore path is pointing to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks` file.
 - f. Leave the Custom Trust Keystore type blank.
 - g. Change the Custom Trust Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
 - h. Re-enter the Custom Trust Keystore Passphrase.
 - i. Click **Save**.
14. Select the **SSL** tab.
 - a. Make sure that Identity and Trust Locations is set to **Keystores**.
 - b. Change the Private Key Alias to `FINHOST2_fusion`.
 - c. Change the Private Key Passphrase to the `keypassword`, as described in the second bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
 - d. Re-enter the `keypassword` from Step c for the Confirm Private Key Passphrase.
 - e. Click **Save**.
15. Select the **Server Start** tab.

Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

```
-DJDBCProgramName=DS/FinancialDomain/GeneralLedgerServer_2  
-Dserver.group=GeneralLedgerCluster
```

Click **Save**.
16. Select the **Logging** tab, and then select the **HTTP** tab.
17. Do the following:
 - a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.
 - b. Change the rotation type to **By Time**.
 - c. Leave the **Limit number of retained files** option unchecked.

- d. Leave the **Rotate log file on startup** option unchecked.
- e. Click **Save**.
- f. Expand **Advanced**.
- g. Change the format to **Extended**.
- h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri
sc-status sc(X-ORACLE-DMS-ECID)
cs(ECID-Context) cs(Proxy-Remote-User)
cs(Proxy-Client-IP)
```

- i. Click **Save**.

18. Click Activate Changes.

19. Repeat Steps 2 to 18 for all the Managed Servers on this domain.

20. Set the following environment variable on *FINHOST2*:

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/
products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks"
```

21. Stop the domain's Administration Server:

```
FINHOST1> ORACLE_BASE/config/domains/FINHOST1/
FinancialDomain/bin/stopWebLogic.sh
```

22. Restart the domain's Administration Server:

```
FINHOST2> ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin/wlst.sh

FINHOST2> nmConnect(username='<username>', password='<password>',
domainName='FinancialDomain', host='FINHOST1',port='5556',
nmType='ssl', domainDir='ORACLE_BASE/config/domains/FINHOST1/FinancialDomain')

FINHOST2> nmStart('AdminServer')
```

Note: The *username* and *password* used in the `nmConnect` are the Node Manager credentials (username and password) specified when creating the provisioning response file. This is shown in [Figure 5-3](#) in "Using the Provisioning Process to Install Components for an Enterprise Deployment".

23. Run the newly created Managed Servers:

- a. Log in to the Administration Server:
`http://fininternal.mycompany.com:7777/console.`
- b. Navigate to **FinancialDomain > Environment > Servers > Control**.
- c. Select the newly created Managed Servers and click **Start**.
- d. Navigate to **FinancialDomain > Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.

8.6 Oracle HTTP Server Configuration

To configure Oracle HTTP Server:

1. On *WEBHOST1*:
 - a. Change directory to *ORACLE_BASE/config/CommonDomain_webtier/config/OHS/ohs1/moduleconf*.
 - b. Copy *FusionVirtualHost_fin.conf* to *FusionVirtualHost_fin.conf.org*.
2. Edit the *FusionVirtualHost_fin.conf* file, adding the scaled-out host and port to all the WebLogic Application Clusters. Add this to both the Internal and External part of the *FusionVirtualHost_fin.conf* file. [Example 8–1](#) shows sample code for *GeneralLedgerServer*.

Notes:

- Do not add these values for Oracle Enterprise Manager, Oracle WebLogic Server Administration Console, or Oracle Authorization Policy Manager.
 - If the Managed Servers are running on VIPs, replace *FINHOST1* and *FINHOST2* with the VIP addresses in [Example 8–1](#).
-

Example 8–1 Sample "GeneralLedgerServer" Code

```
<Location /GeneralLedger>
  SetHandler weblogic-handler
  WebLogicCluster <FINHOST1:port>,<FINHOST2:port>
</Location>
```

3. Repeat Step 2 for all applications.
4. Restart Oracle HTTP Server: cd to *ORACLE_BASE/config/CommonDomain_webtier/bin* and enter the following:

```
WEBHOST1> ./opmnctl stopall
WEBHOST1> ./opmnctl startall
```
5. Repeat Steps 1 through 4 on *WEBHOST2*.

8.7 Configuring Server Migration for the Managed Servers

Server migration is required for proper failover of Oracle Fusion Financials components in the event of failure in any of the *FINHOST1* and *FINHOST2* nodes. For more information, see [Chapter 18, "Setting Up Server Migration for an Enterprise Deployment."](#)

8.8 Validating the System

You should verify URLs to ensure that the appropriate routing and failover are working.

To verify the URLs:

1. Log in to the FinancialDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on *FINHOST1* while the Managed Servers on *FINHOST2* are running.
2. Access the following URLs to verify that routing and failover are functioning properly. (Ensure the log in prompt is visible.)
 - <https://finexternal.mycompany.com/ledger/faces/JournalEntryPage>

- <https://finexternal.mycompany.com/payables/faces/InvoiceWorkbench>
 - <https://finexternal.mycompany.com/receivables/faces/ReceiptsWorkArea>
 - <https://finexternal.mycompany.com/receivables/faces/TransactionsWorkArea>
3. Log in to the FinancialDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on *FINHOST2*.
 4. Start the Managed Servers on *FINHOST1*.
 5. Repeat Step 2. (Ensure the log in prompt is visible.)
 6. Start all the Managed Servers on *FINHOST2* and verify that they are running on *FINHOST1* and *FINHOST2*.

Scaling Out the Oracle Fusion Customer Relationship Management Domain

This chapter describes how to scale out the Oracle Fusion Customer Relationship Management domain.

This chapter includes the following topics:

- [Section 9.1, "Overview of the Oracle Fusion Customer Relationship Management Domain"](#)
- [Section 9.2, "Prerequisites for Scaling Out the Oracle Fusion Customer Relationship Management Domain"](#)
- [Section 9.3, "Adding a New Machine in the Oracle WebLogic Server Console"](#)
- [Section 9.4, "Packing and Unpacking the Managed Server Domain Home"](#)
- [Section 9.5, "Cloning Managed Servers and Assigning Them to FINHOST2"](#)
- [Section 9.6, "Oracle HTTP Server Configuration"](#)
- [Section 9.7, "Configuring Server Migration for the Managed Servers"](#)
- [Section 9.8, "Validating the System"](#)

9.1 Overview of the Oracle Fusion Customer Relationship Management Domain

The Oracle Fusion Customer Relationship Management application is a very distributed and modularized one. Applications within Oracle Fusion Customer Relationship Management, which are deployed on the domain, are the following:

- Contract Management
- CRM Analytics
- CRM Common

In addition to the applications, the Oracle Fusion Customer Relationship Management domain also contains Oracle Fusion Customer Relationship Management Analytics, which is the Oracle BI Enterprise Edition broker application that interfaces with Oracle Application Development Framework, Oracle BI Enterprise Edition, and Oracle Data Integrator agent for data import flow.

[Figure 2–4 in Chapter 2, "Introduction to the Enterprise Deployment Reference Topologies,"](#) shows the topology for the Oracle Fusion Customer Relationship Management domain within the overall reference enterprise deployment topology.

9.2 Prerequisites for Scaling Out the Oracle Fusion Customer Relationship Management Domain

Before you begin, ensure the following:

- Node Manager has been started in the Secure Sockets Layer (SSL) mode by following the instructions in [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"](#)
- You are starting with a clean machine if it is the first time it is being used for a scale out
- The `/etc/hosts` file has proper entries. To verify, ping this machine with the fully qualified name of the machine
- The user created on `FINHOST2` should be the same as the user on `FINHOST1`
- The directory structure `/u01/oracle` is mounted to same shared file system as `FINHOST1`
- The directory structure `/u02/local/oracle/config` on `FINHOST2` has been created
- The initial Oracle Fusion Financials deployment on `FINHOST1` has already been done and verified by provisioning

9.3 Adding a New Machine in the Oracle WebLogic Server Console

To add a new machine:

1. Log in to the Administration Server:
`http://crminternal.mycompany.com:7777/console`.
2. Navigate to **CRMDomain > Environment > Machines**.
LocalMachine is located in the right-hand pane.
3. In the left-hand pane, click **Lock & Edit**.
4. In the right-hand pane, first click **New** to add the remote machine, and then specify the following:
 - Name - enter `FINHOST2`
 - Machine operating system - Unix
5. Click **Next**.
6. In the window that opens, set the following attributes:
 - Type - SSL
 - Listen Address - `<FINHOST2>`
7. Click **Finish** and activate the changes.

Note: The "localhost" default value here is wrong.

Note: If you get an error when activating the changes, see [Section 20.8.18, "Administration Console Redirects from Internal URL to Container URL after Activation"](#) for the temporary solution.

9.4 Packing and Unpacking the Managed Server Domain Home

Since the *FINHOST1* domain directory file system is also available from *FINHOST2*, both the pack and unpack commands can be executed from *FINHOST2*.

To pack and unpack the Managed Server domain home:

1. Change directory to *ORACLE_BASE*/products/fusionapps/oracle_common/common/bin.
2. Run the pack command:

```
FINHOST2> ./pack.sh -managed=true -domain=ORACLE_BASE/config/domains/  
FINHOST1/CRMDomain -template=ORACLE_BASE/user_templates/  
CRMDomain_managed.jar -template_name="CRM_Managed_Server_Domain"
```

3. Ensure that */u02/local/oracle/config/domains/FINHOST2/CRMDomain* is empty, and then run the unpack command:

```
FINHOST2> ./unpack.sh -domain=/u02/local/oracle/config/domains/  
FINHOST2/CRMDomain -template=ORACLE_BASE/user_templates/CRMDomain_managed.jar
```

Here, *ORACLE_BASE* is shared, and */u02/local* is local to *FINHOST2*.

9.5 Cloning Managed Servers and Assigning Them to FINHOST2

To add a Managed Server and assign it to *FINHOST2*:

1. Log in to the Administration Server:
<http://crminternal.mycompany.com:7777/console>.
2. Navigate to **FinancialDomain > Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the *Managed_Server* checkbox (for example, **ContractManagementServer_1**) and then click **Clone**.
5. Specify the following server identity attributes:
 - Server Name - *ContractManagementServer_2*

Note: To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to "_2".

- Server Listen Address - *<FINHOST2>*
- Server Listen Port - leave "as is"

Note: For Oracle SOA Suite server, add a port value that is different than the *soa_server1* server value. This will help in server migration.

6. Click **OK**.

You now should see the newly cloned sales server, *ContractManagementServer_2*.

7. Click **ContractManagementServer_2** and change the following attributes:
 - Machine - <FINHOST2>
 - Cluster Name - accept the default, ContractManagementCluster

Note: Ensure that this cluster name is the same as the cluster name of the original Managed Server.

8. Click **Save** and then **Activate Changes**.
9. Navigate to **CRMDomain > Environment > Servers**.
10. From the **Name** column, click the **ContractManagementServer_2** scaled-out server link.
11. Click **Lock & Edit**, and then select the **Configuration** tab.
12. Select the **Keystores** tab, and ensure that the keystores value is **Custom Identity and Custom Trust**.
13. Do the following:
 - a. Change the Custom Identity Keystore path to point to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/FINHOST2_fusion_identity.jks` file.
 - b. Leave the Custom Identity Keystore type blank.
 - c. Change the Custom Identity Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
 - d. Re-enter the Confirm Custom Identity Keystore Passphrase.
 - e. Ensure that the Confirm Custom Trust Keystore path is pointing to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks` file.
 - f. Leave the Custom Trust Keystore type blank.
 - g. Change the Custom Trust Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
 - h. Re-enter the Custom Trust Keystore Passphrase.
 - i. Click **Save**.
14. Select the **SSL** tab.
 - a. Make sure that Identity and Trust Locations is set to **Keystores**.
 - b. Change the Private Key Alias to `FINHOST2_fusion`.
 - c. Change the Private Key Passphrase to the `keypassword`, as described in the second bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
 - d. Re-enter the `keypassword` from Step c for the Confirm Private Key Passphrase.
 - e. Click **Save**.
15. Select the **Server Start** tab.

Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

```
-DJDBCProgramName=DS/CRMDomain/ContractManagementServer_2
-Dserver.group=ContractManagementCluster
```

Click **Save**.

16. Select the **Logging** tab, and then select the **HTTP** tab.

17. Do the following:

- a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.
- b. Change the rotation type to **By Time**.
- c. Leave the **Limit number of retained files** option unchecked.
- d. Leave the **Rotate log file on startup** option unchecked.
- e. Click **Save**.
- f. Expand **Advanced**.
- g. Change the format to **Extended**.
- h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri
sc-status sc(X-ORACLE-DMS-ECID)
cs(ECID-Context) cs(Proxy-Remote-User)
cs(Proxy-Client-IP)
```

- i. Click **Save**.

18. Click **Activate Changes**.

19. Repeat Steps 2 to 18 for all the Managed Servers on this domain.

20. Set the following environment variable on *FINHOST2*:

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/
products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks"
```

21. Stop the domain's Administration Server:

```
FINHOST1> ORACLE_BASE/config/domains/FINHOST1/CRMDomain/bin/stopWebLogic.sh
```

22. Restart the domain's Administration Server:

```
FINHOST2> ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin/wlst.sh
```

```
FINHOST2> nmConnect(username='username', password='password',
domainName='CRMDomain', host='FINHOST1',port='5556',
nmType='ssl', domainDir='ORACLE_BASE/config/domains/FINHOST1/CRMDomain')
```

```
FINHOST2> nmStart('AdminServer')
```

Note: The *username* and *password* used in the `nmConnect` are the Node Manager credentials (username and password) specified when creating the provisioning response file. This is shown in [Figure 5-3](#) in "Using the Provisioning Process to Install Components for an Enterprise Deployment".

23. Run the newly created Managed Servers:

- a. Log in to the Administration Server:
`http://crminternal.mycompany.com:7777/console.`
- b. Navigate to **CRMDomain > Environment > Servers > Control.**
- c. Select the newly created Managed Servers and click **Start.**
- d. Navigate to **CRMDomain > Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.

9.6 Oracle HTTP Server Configuration

To configure Oracle HTTP Server:

1. On *WEBHOST1*:
 - a. Change directory to `ORACLE_BASE/config/CommonDomain_webtier/config/OHS/ohs1/moduleconf.`
 - b. Copy `FusionVirtualHost_crm.conf` to `FusionVirtualHost_crm.conf.org.`
2. Edit the `FusionVirtualHost_crm.conf` file, adding the scaled-out host and port to all the WebLogic Application Clusters. Add this to both the Internal and External part of the `FusionVirtualHost_crm.conf` file. [Example 9-1](#) shows sample code for `ContactManagementServer`.

Notes:

- Do not add these values for Oracle Enterprise Manager, Oracle WebLogic Server Administration Console, or Oracle Authorization Policy Manager.
 - If the Managed Servers are running on VIPs, replace *FINHOST1* and *FINHOST2* with the VIP addresses in [Example 9-1](#).
-

Example 9-1 Sample "ContractManagementServer" Code

```
<Location /contractManagement>
  SetHandler weblogic-handler
  WebLogicCluster <FINHOST1:port>,<FINHOST2:port>
</Location>
```

3. Repeat Step 2 for all applications.
4. Restart Oracle HTTP Server: `cd` to `ORACLE_BASE/config/CommonDomain_webtier/bin` and enter the following:


```
WEBHOST1> ./opmnctl stopall
WEBHOST1> ./opmnctl startall
```
5. Repeat Steps 1 through 4 on *WEBHOST2*.

9.7 Configuring Server Migration for the Managed Servers

Server migration is required for proper failover of Oracle Fusion Financials components in the event of failure in any of the *FINHOST1* and *FINHOST2* nodes. For more information, see [Chapter 18, "Setting Up Server Migration for an Enterprise Deployment."](#)

9.8 Validating the System

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

To verify the URLs:

1. Log in to the CRMDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on *FINHOST1* while the Managed Servers on *FINHOST2* are running.
2. Access the following URLs to verify that routing and failover are functioning properly. (Ensure the log in prompt is visible.)
 - <https://crmexternal.mycompany.com/contractManagement/faces/ContractsDashboard>
3. Log in to the CRMDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on *FINHOST2*.
4. Start the Managed Servers on *FINHOST1*.
5. Repeat Step 2. (Ensure the log in prompt is visible.)
6. Start all the Managed Servers on *FINHOST2* and verify that they are running on *FINHOST1* and *FINHOST2*.

Scaling Out the Oracle Fusion Common Domain

This chapter describes how to scale out the Oracle Fusion Common domain.

This chapter includes the following topics:

- [Section 10.1, "Overview of the Oracle Fusion Common Domain"](#)
- [Section 10.2, "Prerequisites for Scaling Out the Oracle Fusion Common Domain"](#)
- [Section 10.3, "Adding a New Machine in the Oracle WebLogic Server Console"](#)
- [Section 10.4, "Scaling Out Oracle WebCenter Content"](#)
- [Section 10.5, "Packing and Unpacking the Managed Server Domain Home"](#)
- [Section 10.6, "Cloning Managed Servers and Assigning Them to FINHOST2"](#)
- [Section 10.7, "Oracle HTTP Server Configuration"](#)
- [Section 10.8, "Configuring Server Migration for the Managed Servers"](#)
- [Section 10.9, "Validating the System"](#)

10.1 Overview of the Oracle Fusion Common Domain

The Oracle Fusion Common domain is shared by all Oracle Fusion Applications product families. Oracle Fusion Financials implementation is dependent on the Oracle Fusion Common domain for the following components:

- Oracle Fusion Functional Setup Manager, for all setup task flows
- Help Portal, for centralized help
- Home page application, which has the Oracle Fusion Financials home page and launch pad
- Oracle WebCenter Content, to store all marketing collateral as well as all attachments. Import flow also uses WebCenter Content to stage the CSV files that the user uploads
- Oracle WebCenter Content: Imaging, for end-to-end management of document images within enterprise business processes
- Oracle Secure Enterprise Search
- Oracle WebCenter Community Space and forums
- Oracle WebLogic Communication Services (OWLCS) and Oracle WebLogic SIP Server

Figure 2–5 in Chapter 2, "Introduction to the Enterprise Deployment Reference Topologies," shows the topology for the Oracle Fusion Common domain within the overall reference enterprise deployment topology.

10.2 Prerequisites for Scaling Out the Oracle Fusion Common Domain

Before you begin, ensure the following:

- Node Manager has been started in the Secure Sockets Layer (SSL) mode by following the instructions in Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"
- You are starting with a clean machine if it is the first time it is being used for a scale out
- The `/etc/hosts` file has proper entries. To verify, ping this machine with the fully qualified name of the machine
- The user created on *FINHOST2* should be the same as the user on *FINHOST1*
- The directory structure `/u01/oracle` is mounted to same shared file system as *FINHOST1*
- The directory structure `/u02/local/oracle/config` on *FINHOST2* has been created
- The initial Oracle Fusion Financials deployment on *FINHOST1* has already been done and verified by provisioning

10.3 Adding a New Machine in the Oracle WebLogic Server Console

To add a new machine:

1. Log in to the Administration Server:
`http://commoninternal.mycompany.com:7777/console.`
 2. Navigate to **CommonDomain > Environment > Machines**.
LocalMachine is located in the right-hand pane.
 3. In the left-hand pane, click **Lock & Edit**.
 4. In the right-hand pane, first click **New** to add the remote machine, and then specify the following:
 - Name - enter *FINHOST2*
 - Machine operating system - Unix
 5. Click **Next**.
 6. In the window that opens, set the following attributes:
 - Type - SSL
 - Listen Address - `<FINHOST2>`
-
- Note:** The "localhost" default value here is wrong.
-
- Listen port - 5556
 7. Click **Finish** and activate the changes.

Note: If you get an error when activating the changes, see [Section 20.8.18, "Administration Console Redirects from Internal URL to Container URL after Activation"](#) for the temporary solution.

10.4 Scaling Out Oracle WebCenter Content

Scaling out WebCenter Content involves two tasks:

- [Creating a Common Location for the WebCenter Content Managed Servers](#)
- [Configuring Oracle WebCenter Content: Imaging](#)

10.4.1 Creating a Common Location for the WebCenter Content Managed Servers

Do the following:

1. Ensure that the UCM_server1 Managed Server is functioning properly. You should be able to access and log in to the following:
 - `http://FINHOST1:7012/cs`
2. Shut down the UCM_server1 Managed Server:
 - a. Log in to the Oracle WebLogic Server Administration Console (`http://commoninternal.mycompany.com:7777/console`).
 - b. In the Domain Structure window, first navigate to **Environment > Servers**, and then select the **Control** tab.
 - c. Select the **UCM_server1** checkbox.
 - d. Click **Shutdown** and then **Force Shutdown Now**.
3. Copy *FINHOST1* `/u02/local/oracle/config/domains/FINHOST1/CommonDomain/ucm/cs` directory from the local to the shared location: *ORACLE_BASE/config/domains/FINHOST1/CommonDomain/ucm/cs*.
4. In the *ORACLE_BASE/config/domains/FINHOST1/CommonDomain/ucm/cs/bin/intradoc.cfg* file, create the variables `IntradocDir`, `vaultDir`, and `weblayoutDir` so that they point to the shared location, *ORACLE_BASE/config/domains/FINHOST1/CommonDomain/ucm/cs*.
5. Ensure that the edits you made in Step 4 you also make to the `intradoc.cfg` file in `/u02/local/oracle/config/domains/FINHOST1/CommonDomain/ucm/cs/bin`.
6. Start the UCM_server1 Managed Server.

10.4.2 Configuring Oracle WebCenter Content: Imaging

This section describes the additional steps you must perform in order to complete the Oracle WebCenter Content scale out.

This section includes the following topics:

- [Section 10.4.2.1, "Prerequisite"](#)
- [Section 10.4.2.3, "Configuring a JMS Persistence Store"](#)
- [Section 10.4.2.4, "Configuring a Default Persistence Store for Transaction Recovery"](#)

- [Section 10.4.2.5, "Adding the Oracle Imaging Server Listen Addresses to the List of Allowed Hosts in Oracle WebCenter Content"](#)
- [Section 10.4.2.6, "Creating a Connection to Oracle WebCenter Content"](#)

10.4.2.1 Prerequisite

Before proceeding with the configuration, ensure that you have performed the procedures in [Section 10.5, "Packing and Unpacking the Managed Server Domain Home"](#) and in [Section 10.6, "Cloning Managed Servers and Assigning Them to FINHOST2"](#).

10.4.2.2 Configuring the WebCenter Content Server

To configure the WebCenter Content server, do the following:

1. Navigate to `http://FINHOST1:7012/cs` and select **Administration > Providers**.

Note: `ibrprovider` is already defined in this list.

2. Add a new outgoing provider:

- a. Click **Add**.
- b. Set the values to match the values of `ibrprovider`.

Note: The value for the new outgoing `ibrprovider` must differ from the value of the default `ibrprovider`.

- c. Set the server host name to the second host address's `FINHOST2` IP address.
 - d. Set the server socket port to `7035`.
 - e. Assign unique values to Provider Name, Provider Description, Server Host Name, Server Port, Instance Name, and Relative Web Root.
 - f. Restart the `UCM_server1` and `UCM_server2` Managed Servers.
3. Create a `COMMONUCMVH1` TCP VIP with an unused port on the load-balancing router (LBR) with `FINHOST1:7012` and `FINHOST2:7012` as its members.

After scaling out the Oracle WebCenter Portal Managed Server, do the following:

1. Log in to: `http://commoninternal.mycompany.com:7777/em`.

Note: If you don't see WebCenter Content after logging in to Oracle Enterprise Manager, bounce the WebCenter Content Managed Servers.

2. Navigate to **WebCenter > Spaces > webcenter (1.1.*.*) (wc_spaces) > WebCenter Portal** (top left or right pane) > **Settings > Service configuration**.

Click **Content Repository**.

3. Highlight **WebCenter-UCM** and click **Edit**.
4. Select **Socket** and enter `COMMONUCMVH1` as the host.
5. Restart the Oracle WebCenter Portal Managed Servers.

10.4.2.3 Configuring a JMS Persistence Store

You must configure the location for all persistence stores to a directory visible from both nodes. Change all persistent stores to use this shared base directory.

To configure the file store for *FINHOST2*:

1. Log in to the Oracle WebLogic Server Administration Console (<http://commoninternal.mycompany.com:7777/console>).
2. In the Domain Structure window, expand the **Services** node and then click the **Persistence Stores** node.
The Summary of Persistent Stores page displays.
3. In the Change Center, click **Lock & Edit**.
4. Click **New**, and then **Create File Store**.
5. Enter the following directory information:
 - **Name:** For example, `IPMJMSFileStore_auto_2`
 - **Target:** `IPM_server1`
 - **Directory:** `ORACLE_BASE/config/domains/FINHOST1/CommonDomain`
6. Click **Save** and **Activate Changes**.
7. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Servers** node.
The Summary of JMS Servers page displays.
8. Click **Lock & Edit**, then click **New**.
9. Enter a name (for example, `IpmJmsServer_1`), then select **IPMJMSFileStore_auto_2** in the Persistence Store dropdown list.
10. Click **Next**.
11. Select **IPM_server2** as the target.
12. Click **Finish** and **Activate Changes**.

10.4.2.4 Configuring a Default Persistence Store for Transaction Recovery

Each server has a transaction log which stores information about committed transactions that are coordinated by the server that may not have been completed. Oracle WebLogic Server uses this transaction log for recovery from system crashes or network failures. To leverage the migration capability of the Transaction Recovery Service for the servers within a cluster, store the transaction log in a location accessible to a server and its backup servers.

Note: Preferably, this location should be a dual-ported SCSI disk or on a Storage Area Network (SAN).

To set the location for the default persistence store:

1. Log in to the Oracle WebLogic Server Administration Console (<http://commoninternal.mycompany.com:7777/console>).
2. In the Change Center, click **Lock & Edit**.
3. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node.

The Summary of Servers page displays.

4. Click the name of the server (represented as a hyperlink) in the **IPM_server1** table. The settings page for the selected server opens with the **Configuration** tab active.
5. Open the **Services** tab.
6. In the Default Store section of the page, enter the path to the folder where the default persistent stores will store its data files. For example:

```
FINHOST1> ORACLE_BASE/config/domains/FINHOST1/CommonDomain/tlogs
```
7. Click **Save**.
8. Repeat Steps 1 through 7 for the **IPM_server2** Managed Server.
9. Click **Activate Changes**.
10. Restart the Managed Servers to activate the changes (ensure that Node Manager is up and running):
 - a. Log in to the Oracle WebLogic Server Administration Console (<http://commoninternal.mycompany.com:7777/console>).
 - b. In the Summary of Servers screen, select the **Control** tab.
 - c. Select **IPM_server1** and **IPM_server2** in the table and then click **Shutdown**.
 - d. Restart the **IPM_server1** and **IPM_server2** Managed Servers.

Notes:

- To enable migration of the Transaction Recovery service, specify a location on a persistent storage solution that is available to other servers in the cluster. Both **IPM_server1** and **IPM_server2** must be able to access this directory.
 - Ensure the following the path exists on your machine:
`/usr/share/X11/fonts/TTF.`
-

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

Perform these steps to add the host names of the **IPM_server1** and **IPM_server2** Managed Servers to the `SocketHostNameSecurityFilter` parameter list:

1. Open the following file in a text editor:

```
ORACLE_BASE/config/domains/FINHOST1/CommonDomain/ucm/cs/config/config.cfg
```

2. Remove or comment out the following line:

```
SocketHostAddressSecurityFilter=127.0.0.1|FINHOST1|FINHOST2|0.0.0.0.0.0.1
```

3. Add the following two lines to include the **IPM_server1** and **IPM_server2** listen addresses to the list of addresses that are allowed to connect to Oracle WebCenter Content:

```
SocketHostAddressSecurityFilter=localhost|localhost.mycompany.com|FINHOST1|  
FINHOST2|COMMONIPMVH1|COMMONIPMVH2
```

```
AlwaysReverseLookupForHost=Yes
```

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

10.4.2.6 Creating a Connection to Oracle WebCenter Content

To create a connection to Oracle WebCenter Content Server:

1. Log in to the IPM_server1 Imaging console at `https://commonexternal.mycompany.com/imaging`.
2. In the left-hand pane, click **Manage Connections**, and then **Create Content Server Connection**.
3. Enter a name and description for the new connection, and then click **Next**.
4. In the Connection Settings screen, do the following:
 - Make sure the **Use Local Content Server** checkbox is not selected.
 - Set the Content Server port to 7034.
The port value should be the value of the `IntradocServerPort` from `ORACLE_BASE/config/domains/FINHOST1/CommonDomain/ucm/cs/config/config.cfg`.
 - Add two servers to the Content Server pool:
 - `FINHOST1: 7034`
 - `FINHOST2: 4444`

Click **Next**.
5. In the Connection Security screen, leave the default selections for the WebLogic user, and then click **Next**.
6. Review the connection details and click **Submit**.

10.5 Packing and Unpacking the Managed Server Domain Home

Since the `FINHOST1` domain directory file system is also available from `FINHOST2`, both the `pack` and `unpack` commands can be executed from `FINHOST2`.

To pack and unpack the Managed Server domain home:

1. Change directory to `ORACLE_BASE/products/fusionapps/oracle_common/common/bin`.
2. Run the `pack` command:

```
FINHOST2> ./pack.sh -managed=true -domain=ORACLE_BASE/config/domains/
FINHOST1/CommonDomain -template=ORACLE_BASE/user_templates/
CommonDomain_managed.jar -template_name="Common_Managed_Server_Domain"
```

3. Ensure that `/u02/local/oracle/config/domains/FINHOST2/CommonDomain` is empty, and then run the `unpack` command:

```
FINHOST2> ./unpack.sh -domain=/u02/local/oracle/config/domains/FINHOST2/
CommonDomain -template=ORACLE_BASE/user_templates/CommonDomain_managed.jar
```

Here, `ORACLE_BASE` is shared, and `/u02/local` is local to `FINHOST2`.

10.6 Cloning Managed Servers and Assigning Them to FINHOST2

To add a Managed Server and assign it to *FINHOST2*:

1. Log in to the Administration Server:
`http://commoninternal.mycompany.com:7777/console.`
2. Navigate to **CommonDomain > Environment > Servers.**
3. Switch to **Lock & Edit** mode.
4. Select the *Managed_Server* checkbox (for example, **HomePageServer_1**) and then click **Clone.**
5. Specify the following Server Identity attributes:

- Server Name - HomePageServer_2

Note: To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to "_2".

- Server Listen Address - *<FINHOST2>*
- Server Listen Port - leave "as is"

Note: For Oracle SOA Suite server, add a port value that is different than the `soa_server1` server value. This will help in server migration.

6. Click **OK.**

You now should see the newly cloned sales server, `HomePageServer_2`.

7. Click **HomePageServer_2** and change the following attributes:

- Machine - *<FINHOST2>*
- Cluster Name - accept the default, `HomePageCluster`

Note: Ensure that this cluster name is the same as the cluster name of the original Managed Server.

8. Click **Save** and then **Activate Changes.**
9. Navigate to **CommonDomain > Environment > Servers.**
10. From the **Name** column, click the **HomepageServer_2** scaled-out server link.
11. Click **Lock & Edit**, and then select the **Configuration** tab.
12. Select the **Keystores** tab, and then ensure that the keystores value is **Custom Identity and Custom Trust.**
13. Do the following:

- a. Change the Custom Identity Keystore path to point to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/FINHOST2_fusion_identity.jks` file.
 - b. Leave the Custom Identity Keystore type blank.
 - c. Change the Custom Identity Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
 - d. Re-enter the Confirm Custom Identity Keystore Passphrase.
 - e. Ensure that the Confirm Custom Trust Keystore path is pointing to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks` file.
 - f. Leave the Custom Trust Keystore type blank.
 - g. Change the Custom Trust Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
 - h. Re-enter the Custom Trust Keystore Passphrase.
 - i. Click **Save**.
14. Select the **SSL** tab.
- a. Make sure that Identity and Trust Locations is set to **Keystores**.
 - b. Change the Private Key Alias to `FINHOST2_fusion`.
 - c. Change the Private Key Passphrase to the `keypassword`, as described in the second bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
 - d. Re-enter the `keypassword` from Step c for the Confirm Private Key Passphrase.
 - e. Click **Save**.
15. Select the **Server Start** tab.
- Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:
- ```
-DJDBCProgramName=DS/CommonDmain/HomePageServer_2
-Dserver.group=HomePageCluster
```
- Click **Save**.
16. Select the **Logging** tab, and then select the **HTTP** tab.
17. Do the following:
- a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.
  - b. Change the rotation type to **By Time**.
  - c. Leave the **Limit number of retained files** option unchecked.
  - d. Leave the **Rotate log file on startup** option unchecked.
  - e. Click **Save**.
  - f. Expand **Advanced**.
  - g. Change the format to **Extended**.

- h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri
sc-status sc (X-ORACLE-DMS-ECID)
cs (ECID-Context) cs (Proxy-Remote-User)
cs (Proxy-Client-IP)
```

- i. Click **Save**.

18. Click **Activate Changes**.

19. Repeat Steps 2 to 18 for all the Managed Servers on this domain.

20. Set the following environment variable on *FINHOST2*:

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/
products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks"
```

21. Stop the domain's Administration Server:

```
FINHOST1> ORACLE_BASE/config/domains/FINHOST1/CommonDomain/bin/stopWebLogic.sh
```

22. Restart the domain's Administration Server:

```
FINHOST2> ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin/wlst.sh

FINHOST2> nmConnect(username='<username>', password='<password>',
domainName='CommonDomain', host='FINHOST1',port='5556',
nmType='ssl', domainDir='ORACLE_BASE/config/domains/FINHOST1/CommonDomain')

FINHOST2> nmStart('AdminServer')
```

---

**Note:** The *username* and *password* used in the `nmConnect` are the Node Manager credentials (username and password) specified when creating the provisioning response file. This is shown in [Figure 5–3](#) in "Using the Provisioning Process to Install Components for an Enterprise Deployment".

---

23. For the `wlcs_sipstate2` scaled-out server only, do the following:

- a. Change directory to:

```
ORACLE_BASE/config/domains/FINHOST1/CommonDomain/config/custom
```

- b. In the `datatier.xml` file, after the following line:

```
<server-name>wlcs_sipstate1</server-name>

add

<server-name>wlcs_sipstate2</server-name>
```

24. For Oracle WebCenter Content: Imaging scaleout only: Before starting the `IPM_server2` server, perform the steps listed in [Section 10.4.2.3, "Configuring a JMS Persistence Store."](#)

25. In the `intradoc.cfg` file located at

```
/u02/local/oracle/config/domains/FINHOST2/CommonDomain/ucm/cs/bin,
create the variables IntradocDir, vaultDir, and weblayoutDir so that they point
to the shared location, ORACLE_
BASE/config/domains/CRMHOST1/CommonDomain/ucm/cs.
```

26. Run the newly created Managed Servers:
  - a. Log in to the Administration Server:  
`http://commoninternal.mycompany.com:7777/console.`
  - b. Navigate to **CommonDomain > Environment > Servers > Control**.
  - c. Select the newly created Managed Servers and click **Start**.
  - d. Navigate to **CommonDomain > Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.
27. For additional scale-out instructions for Oracle WebCenter Content, see [Section 10.4](#).

## 10.7 Oracle HTTP Server Configuration

To configure Oracle HTTP Server:

1. On *WEBHOST1*:
  - a. Change directory to `ORACLE_BASE/config/CommonDomain_webtier/config/OHS/ohs1/moduleconf`.
  - b. Copy `FusionVirtualHost_fs.conf` to `FusionVirtualHost_fs.conf.org`.
2. Edit the `FusionVirtualHost_fs.conf` file, adding the scaled-out host and port to all the WebLogic Application Clusters. Add this to both the Internal and External part of the `FusionVirtualHost_fs.conf` file. [Example 10–1](#) shows sample code for `HomePageServer`.

---



---

### Notes:

- Do not add these values for Oracle Enterprise Manager, Oracle WebLogic Server Administration Console, or Oracle Authorization Policy Manager.
  - If the Managed Servers are running on VIPs, replace *FINHOST1* and *FINHOST2* with the VIP addresses in [Example 10–1](#).
- 
- 

### Example 10–1 Sample "HomePageServer" Code

```
<Location /HomePage>
 SetHandler weblogic-handler
 WebLogicCluster <FINHOST1:port>,<FINHOST2:port>
</Location>
```

3. Repeat Step 2 for all applications.
4. Restart Oracle HTTP Server: `cd` to `ORACLE_BASE/config/CommonDomain_webtier/bin` and enter the following:
 

```
WEBHOST1> ./opmnctl stopall
WEBHOST1> ./opmnctl startall
```
5. Repeat Steps 1 through 4 on *WEBHOST2*.

## 10.8 Configuring Server Migration for the Managed Servers

Server migration is required for proper failover of Oracle Fusion Financials components in the event of failure in any of the *FINHOST1* and *FINHOST2* nodes. For

more information, see [Chapter 18, "Setting Up Server Migration for an Enterprise Deployment."](#)

## 10.9 Validating the System

You should verify URLs to ensure that the appropriate routing and failover are working.

To verify the URLs:

1. Log in to the CommonDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on *FINHOST1* while the Managed Servers on *FINHOST2* are running.
2. Access the following URLs to verify that routing and failover are functioning properly. (Ensure the log in prompt is visible.)
  - <https://commonexternal.mycompany.com/helpPortal/faces/AtkHelpPortalMain>
  - <https://commonexternal.mycompany.com/homePage/faces/AtkHomePageWelcome>
3. Log in to the CommonDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on *FINHOST2*.
4. Start the Managed Servers on *FINHOST1*.
5. Repeat Step 2. (Ensure the log in prompt is visible.)
6. Start all the Managed Servers on *FINHOST2* and verify that they are running on *FINHOST1* and *FINHOST2*.

---

# Scaling Out the Oracle Fusion Human Capital Management Domain

This chapter describes how to scale out the Oracle Fusion Human Capital Management domain.

This chapter includes the following topics:

- [Section 11.1, "Overview of the Oracle Fusion Human Capital Management Domain"](#)
- [Section 11.2, "Prerequisites for Scaling Out the Oracle Fusion Human Capital Management Domain"](#)
- [Section 11.3, "Adding a New Machine in the Oracle WebLogic Server Console"](#)
- [Section 11.4, "Packing and Unpacking the Managed Server Domain Home"](#)
- [Section 11.5, "Cloning Managed Servers and Assigning Them to FINHOST2"](#)
- [Section 11.6, "Oracle HTTP Server Configuration"](#)
- [Section 11.7, "Configuring Server Migration for the Managed Servers"](#)
- [Section 11.8, "Validating the System"](#)

## 11.1 Overview of the Oracle Fusion Human Capital Management Domain

The Oracle Fusion Human Capital Management domain provides the user-management flow needed to create a user, which is executed via Oracle Fusion Human Capital Management/Oracle Identity Management integration. The flow is available as part of Customer Data Management.

[Figure 2–6 in Chapter 2, "Introduction to the Enterprise Deployment Reference Topologies,"](#) shows the topology for the Oracle Fusion Human Capital Management domain within the overall reference enterprise deployment topology.

## 11.2 Prerequisites for Scaling Out the Oracle Fusion Human Capital Management Domain

Before you begin, ensure the following:

- Node Manager has been started in the Secure Sockets Layer (SSL) mode by following the instructions in [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"](#)
- You are starting with a clean machine if it is the first time it is being used for a scale out

- The `/etc/hosts` file has proper entries. To verify, ping this machine with the fully qualified name of the machine
- The user created on *FINHOST2* should be the same as the user on *FINHOST1*
- The directory structure `/u01/oracle` is mounted to same shared file system as *FINHOST1*
- The directory structure `/u02/local/oracle/config` on *FINHOST2* has been created
- The initial Oracle Fusion Financials deployment on *FINHOST1* has already been done and verified by provisioning

## 11.3 Adding a New Machine in the Oracle WebLogic Server Console

To add a new machine:

1. Log in to the Administration Server:  
`http://hcminternal.mycompany.com:7777/console.`
2. Navigate to **HCMDomain > Environment > Machines**.  
LocalMachine is located in the right-hand pane.
3. In the left-hand pane, click **Lock & Edit**.
4. In the right-hand pane, first click **New** to add the remote machine, and then specify the following:
  - Name - enter *FINHOST2*
  - Machine operating system - Unix
5. Click **Next**.
6. In the window that opens, set the following attributes:
  - Type - SSL
  - Listen Address - `<FINHOST2>`

---

**Note:** The "localhost" default value here is wrong.

---

- Listen port - 5556
7. Click **Finish** and activate the changes.

---

**Note:** If you get an error when activating the changes, see [Section 20.8.18, "Administration Console Redirects from Internal URL to Container URL after Activation"](#) for the temporary solution.

---

## 11.4 Packing and Unpacking the Managed Server Domain Home

Since the *FINHOST1* domain directory file system is also available from *FINHOST2*, both `pack` and `unpack` commands can be executed from *FINHOST2*.

To pack and unpack the Managed Server domain home:

1. Change directory to `ORACLE_BASE/products/fusionapps/oracle_common/common/bin`.
2. Run the `pack` command:

```
FINHOST2> ./pack.sh -managed=true -domain=ORACLE_
BASE/config/domains/FINHOST1/HCMDomain -template=ORACLE_BASE/user_templates/
HCMDomain_managed.jar -template_name="HCM_Managed_Server_Domain"
```

3. Ensure that `/u02/local/oracle/config/domains/FINHOST2/HCMDomain` is empty, and then run the `FINHOST2` command:

```
FINHOST2> ./unpack.sh -domain=/u02/local/oracle/config/domains/
FINHOST2/HCMDomain -template=ORACLE_BASE/user_templates/HCMDomain_managed.jar
```

Here, `ORACLE_BASE` is shared, and `/u02/local` is local to `FINHOST2`.

## 11.5 Cloning Managed Servers and Assigning Them to FINHOST2

To add a Managed Server and assign it to `FINHOST2`:

1. Log in to the Administration Server:  
`http://hcminternal.mycompany.com:7777/console`
2. Navigate to **HCMDomain > Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the *Managed\_Server* checkbox (for example, **CoreSetupServer\_1**) and then click **Clone**.
5. Specify the following Server Identity attributes:

- Server Name - `CoreSetupServer_2`

---

---

**Note:** To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to `"_2"`.

---

---

- Server Listen Address - `<FINHOST2>`
- Server Listen Port - leave "as is"

---

---

**Note:** For Oracle SOA Suite server, add a port value that is different than the `soa_server1` server value. This will help in server migration.

---

---

6. Click **OK**.

You now should see the newly cloned sales server, `CoreSetupServer_2`.

7. Click **CoreSetupServer\_2** and change the following attributes:

- Machine - `<FINHOST2>`
- Cluster Name - accept the default, `CoreSetupCluster`

---

---

**Note:** Ensure that this cluster name is the same as the cluster name of the original Managed Server.

---

---

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

9. Navigate to **HCMDomain > Environment > Servers**.
10. From the **Name** column, click the **CoreSetupServer\_2** scaled-out server link.
11. Click **Lock & Edit**, and then select the **Configuration** tab.
12. Select the **Keystores** tab, and then ensure that the keystores value is **Custom Identity and Custom Trust**.
13. Do the following:
  - a. Change the Custom Identity Keystore path to point to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/FINHOST2_fusion_identity.jks` file.
  - b. Leave the Custom Identity Keystore type blank.
  - c. Change the Custom Identity Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - d. Re-enter the Confirm Custom Identity Keystore Passphrase.
  - e. Ensure that the Confirm Custom Trust Keystore path is pointing to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks` file.
  - f. Leave the Custom Trust Keystore type blank.
  - g. Change the Custom Trust Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - h. Re-enter the Custom Trust Keystore Passphrase.
  - i. Click **Save**.
14. Select the **SSL** tab.
  - a. Make sure that Identity and Trust Locations is set to **Keystores**.
  - b. Change the Private Key Alias to `FINHOST2_fusion`.
  - c. Change the Private Key Passphrase to the `keypassword`, as described in the second bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - d. Re-enter the `keypassword` from Step c for the Confirm Private Key Passphrase.
  - e. Click **Save**.
15. Select the **Server Start** tab.

Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

```
-DJDBCProgramName=DS/HCMDomain/CoreSetupServer_2
-Dserver.group=CoreSetupCluster
```

Click **Save**.
16. Select the **Logging** tab, and then select the **HTTP** tab.
17. Do the following:
  - a. Change the Log file name to `logs/access.log.%yyyymmdd%`.

- b. Change the rotation type to **By Time**.
- c. Leave the **Limit number of retained files** option unchecked.
- d. Leave the **Rotate log file on startup** option unchecked.
- e. Click **Save**.
- f. Expand **Advanced**.
- g. Change the format to **Extended**.
- h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri
sc-status sc(X-ORACLE-DMS-ECID)
cs(ECID-Context) cs(Proxy-Remote-User)
cs(Proxy-Client-IP)
```

- i. Click **Save**.

**18. Click **Activate Changes**.**

**19. Repeat Steps 2 to 18 for all the Managed Servers on this domain.**

**20. Set the following environment variable on *FINHOST2*:**

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/
products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks"
```

**21. Stop the domain's Administration Server:**

```
FINHOST1> ORACLE_BASE/config/domains/FINHOST1/HCMDomain/bin/stopWebLogic.sh
```

**22. Restart the domain's Administration Server:**

```
FINHOST2> ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin/wlst.sh
```

```
FINHOST2> nmConnect(username='<username>', password='<password>',
domainName='HCMDomain', host='FINHOST1',port='5556',
nmType='ssl', domainDir='ORACLE_BASE/config/domains/FINHOST1/HCMDomain')
```

```
FINHOST2> nmStart('AdminServer')
```

---

**Note:** The *username* and *password* used in the `nmConnect` are the Node Manager credentials (username and password) specified when creating the provisioning response file. This is shown in [Figure 5-3](#) in "Using the Provisioning Process to Install Components for an Enterprise Deployment".

---

**23. Run the newly created Managed Servers:**

- a. Log in to the Administration Server:  
`http://hcminternal.mycompany.com:7777/console.`
- b. Navigate to **HCMDomain > Environment > Servers > Control**.
- c. Select the newly created Managed Servers and click **Start**.
- d. Navigate to **HCMDomain > Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.

## 11.6 Oracle HTTP Server Configuration

To configure Oracle HTTP Server:

1. On *WEBHOST1*:
  - a. Change directory to *ORACLE\_BASE/config/CommonDomain\_webtier/config/OHS/ohs1/moduleconf*.
  - b. Copy *FusionVirtualHost\_hcm.conf* to *FusionVirtualHost\_hcm.conf.org*.
2. Edit the *FusionVirtualHost\_hcm.conf* file, adding the scaled-out host and port to all the WebLogic Application Clusters. Add this to both the Internal and External part of the *FusionVirtualHost\_hcm.conf* file. [Example 11–1](#) shows sample code for *CoreSetupServer*.

---



---

### Notes:

- Do not add these values for Oracle Enterprise Manager, Oracle WebLogic Server Administration Console, or Oracle Authorization Policy Manager.
  - If the Managed Servers are running on VIPs, replace *FINHOST1* and *FINHOST2* with the VIP addresses in [Example 11–1](#).
- 
- 

#### Example 11–1 Sample "CoreSetupServer" Code

```
<Location /hcmCoreSetup>
 SetHandler weblogic-handler
 WebLogicCluster <FINHOST1:port>,<FINHOST2:port>
</Location>
```

3. Repeat Step 2 for all applications.
4. Restart Oracle HTTP Server: cd to *ORACLE\_BASE/config/CommonDomain\_webtier/bin* and enter the following:
 

```
WEBHOST1> ./opmnctl stopall
WEBHOST1> ./opmnctl startall
```
5. Repeat Steps 1 through 4 on *WEBHOST2*.

## 11.7 Configuring Server Migration for the Managed Servers

Server migration is required for proper failover of Oracle Fusion Financials components in the event of failure in any of the *FINHOST1* and *FINHOST2* nodes. For more information, see [Chapter 18, "Setting Up Server Migration for an Enterprise Deployment."](#)

## 11.8 Validating the System

You should verify URLs to ensure that the appropriate routing and failover are working.

To verify the URLs:

1. Log in to the HCMDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on *FINHOST1* while the Managed Servers on *FINHOST2* are running.

2. Access the following URLs to verify that routing and failover are functioning properly. (Ensure the log in prompt is visible.)
  - <https://hcmexternal.mycompany.com/hcmCore/faces/AddPersonUiShellMainPage>
  - <https://hcmexternal.mycompany.com/hcmCore/faces/PersonSearch>
3. Log in to the HCMDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on *FINHOST2*.
4. Start the Managed Servers on *FINHOST1*.
5. Repeat Step 2. (Ensure the log in prompt is visible.)
6. Start all the Managed Servers on *FINHOST2* and verify that they are running on *FINHOST1* and *FINHOST2*.



---

# Scaling Out the Oracle Fusion Supply Chain Management Domain

This chapter describes how to scale out the Oracle Fusion Supply Chain Management domain.

This chapter includes the following topics:

- [Section 12.1, "Overview of the Oracle Fusion Supply Chain Management Domain"](#)
- [Section 12.2, "Prerequisites for Scaling Out the Oracle Fusion Supply Chain Management Domain"](#)
- [Section 12.3, "Adding a New Machine in the Oracle WebLogic Server Console"](#)
- [Section 12.4, "Packing and Unpacking the Managed Server Domain Home"](#)
- [Section 12.5, "Cloning Managed Servers and Assigning Them to FINHOST2"](#)
- [Section 12.6, "Oracle HTTP Server Configuration"](#)
- [Section 12.7, "Configuring Server Migration for the Managed Servers"](#)
- [Section 12.8, "Validating the System"](#)

## 12.1 Overview of the Oracle Fusion Supply Chain Management Domain

Oracle Fusion Financials uses Oracle Fusion Supply Chain Management for products and product groups. The Oracle Fusion Supply Chain Management domain provides the flows to import any existing customer product and product catalog into Oracle Fusion Financials.

[Figure 2–7 in Chapter 2, "Introduction to the Enterprise Deployment Reference Topologies,"](#) shows the topology for the Oracle Fusion Supply Chain Management domain within the overall reference enterprise deployment topology.

## 12.2 Prerequisites for Scaling Out the Oracle Fusion Supply Chain Management Domain

Before you begin, ensure the following:

- Node Manager has been started in the Secure Sockets Layer (SSL) mode by following the instructions in [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"](#)
- You are starting with a clean machine if it is the first time it is being used for a scale out

- The `/etc/hosts` file has proper entries. To verify, ping this machine with the fully qualified name of the machine
- The user created on *FINHOST2* should be the same as the user on *FINHOST1*
- The directory structure `/u01/oracle` is mounted to same shared file system as *FINHOST1*
- The directory structure `/u02/local/oracle/config` on *FINHOST2* has been created
- The initial Oracle Fusion Financials deployment on *FINHOST1* has already been done and verified by provisioning

## 12.3 Adding a New Machine in the Oracle WebLogic Server Console

To add a new machine:

1. Log in to the Administration Server:  
`http://scminternal.mycompany.com:7777/console.`
2. Navigate to **SCMDomain > Environment > Machines.**  
Local Machine is located in the right-hand pane.
3. In the left-hand pane, click **Lock & Edit.**
4. In the right-hand pane, first click **New** to add the remote machine, and then specify the following:
  - Name - enter *FINHOST2*
  - Machine operating system - Unix
5. Click **Next.**
6. In the window that opens, set the following attributes:
  - Type - SSL
  - Listen Address - `<FINHOST2>`

---

**Note:** The "localhost" default value here is wrong.

---

- Listen port - 5556
7. Click **Finish** and activate the changes.

---

**Note:** If you get an error when activating the changes, see [Section 20.8.18, "Administration Console Redirects from Internal URL to Container URL after Activation"](#) for the temporary solution.

---

## 12.4 Packing and Unpacking the Managed Server Domain Home

Since the *FINHOST1* domain directory file system is also available from *FINHOST2*, both `pack` and `unpack` commands can be executed from *FINHOST2*.

To pack and unpack the Managed Server domain home:

1. Change directory to `ORACLE_BASE/products/fusionapps/oracle_common/common/bin.`
2. Run the `pack` command:

```
FINHOST2> ./pack.sh -managed=true -domain=ORACLE_BASE/config/domains/
FINHOST1/SCMDomain -template=ORACLE_BASE/user_templates/
SCMDomain_managed.jar -template_name="SCM_Managed_Server_Domain"
```

3. Ensure that `/u02/local/oracle/config/domains/FINHOST2/SCMDomain` is empty, and then run the unpack command:

```
FINHOST2> ./unpack.sh -domain=/u02/local/oracle/config/domains/FINHOST2/
SCMDomain -template=ORACLE_BASE/user_templates/SCMDomain_managed.jar
```

Here, `ORACLE_BASE` is shared, and `/u02/local` is local to `FINHOST2`.

## 12.5 Cloning Managed Servers and Assigning Them to FINHOST2

To add a Managed Server and assign it to `FINHOST2`:

1. Log in to the Administration Server:  
`http://scminternal.mycompany.com:7777/console.`
2. Navigate to **SCMDomain > Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the *Managed\_Server* checkbox (for example, **CostManagementServer\_1**) and then click **Clone**.
5. Specify the following Server Identity attributes:

- Server Name - `CostManagementServer_2`

---

**Note:** To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to `"_2"`.

---

- Server Listen Address - `<FINHOST2>`
- Server Listen Port - leave "as is"

---

**Note:** For Oracle SOA Suite server, add a port value that is different than the `soa_server1` server value. This will help in server migration.

---

6. Click **OK**.

You now should see the newly cloned sales server, `CostManagementServer_2`.

7. Click **CostManagementServer\_2** and change the following attributes:

- Machine - `<FINHOST2>`
- Cluster Name - accept the default, `CostManagementCluster`

---

**Note:** Ensure that this cluster name is the same as the cluster name of the original Managed Server.

---

8. Click **Save** and then **Activate Changes**.
9. Navigate to **SCMDomain > Environment > Servers**.

10. From the **Name** column, click the **CostManagementServer\_2** scaled-out server link.
11. Click **Lock & Edit**, and then select the **Configuration** tab.
12. Select the **Keystores** tab, and ensure that the keystores value is **Custom Identity and Custom Trust**.
13. Do the following:
  - a. Change the Custom Identity Keystore path to point to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/FINHOST2_fusion_identity.jks` file.
  - b. Leave the Custom Identity Keystore type blank.
  - c. Change the Custom Identity Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - d. Re-enter the Confirm Custom Identity Keystore Passphrase.
  - e. Ensure that the Confirm Custom Trust Keystore path is pointing to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks` file.
  - f. Leave the Custom Trust Keystore type blank.
  - g. Change the Custom Trust Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - h. Re-enter the Custom Trust Keystore Passphrase.
  - i. Click **Save**.
14. Select the **SSL** tab.
  - a. Make sure that Identity and Trust Locations is set to **Keystores**.
  - b. Change the Private Key Alias to `FINHOST2_fusion`.
  - c. Change the Private Key Passphrase to the `keypassword`, as described in the second bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - d. Re-enter the `keypassword` from Step c for the Confirm Private Key Passphrase.
  - e. Click **Save**.
15. Select the **Server Start** tab.

Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

```
-DJDBCProgramName=DS/SCMDomain/CostManagementServer_2
-Dserver.group=CostManagementCluster
```

Click **Save**.
16. Select the **Logging** tab, and then select the **HTTP** tab.
17. Do the following:
  - a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.
  - b. Change the rotation type to **By Time**.

- c. Leave the **Limit number of retained files** option unchecked.
- d. Leave the **Rotate log file on startup** option unchecked.
- e. Click **Save**.
- f. Expand **Advanced**.
- g. Change the format to **Extended**.
- h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri
sc-status sc (X-ORACLE-DMS-ECID)
cs (ECID-Context) cs (Proxy-Remote-User)
cs (Proxy-Client-IP)
```

- i. Click **Save**.

**18. Click *Activate Changes*.**

**19. Repeat Steps 2 to 18 for all the Managed Servers on this domain.**

**20. Set the following environment variable on *FINHOST2*:**

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/
products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks"
```

**21. Stop the domain's Administration Server:**

```
FINHOST1> ORACLE_BASE/config/domains/FINHOST1/SCMDomain/bin/stopWebLogic.sh
```

**22. Restart the domain's Administration Server:**

```
FINHOST2> ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin/wlst.sh
```

```
FINHOST2> nmConnect(username='<username>', password='<password>',
domainName='SCMDomain', host='FINHOST1',port='5556',
nmType='ssl', domainDir='ORACLE_BASE/config/domains/FINHOST1/SCMDomain')
```

```
FINHOST2> nmStart('AdminServer')
```

---

**Note:** The *username* and *password* used in the `nmConnect` are the Node Manager credentials (username and password) specified when creating the provisioning response file. This is shown in [Figure 5–3](#) in "[Using the Provisioning Process to Install Components for an Enterprise Deployment](#)".

---

**23. Run the newly created Managed Servers:**

- a. Log in to the Administration Server:  
`http://scminternal.mycompany.com:7777/console.`
- b. Navigate to **SCMDomain > Environment > Servers > Control**.
- c. Select the newly created Managed Servers and click **Start**.
- d. Navigate to **SCMDomain > Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.

## 12.6 Oracle HTTP Server Configuration

To configure Oracle HTTP Server:

1. On *WEBHOST1*:
  - a. Change directory to *ORACLE\_BASE/config/CommonDomain\_webtier/config/OHS/ohs1/moduleconf*.
  - b. Copy *FusionVirtualHost\_scm.conf* to *FusionVirtualHost\_scm.conf.org*.
2. Edit the *FusionVirtualHost\_scm.conf* file, adding the scaled-out host and port to all the WebLogic Application Clusters. Add this to both the Internal and External part of the *FusionVirtualHost\_scm.conf* file. [Example 12–1](#) shows sample code for *CostManagementServer*.

---

**Notes:**

- Do not add these values for Oracle Enterprise Manager, Oracle WebLogic Server Administration Console, or Oracle Authorization Policy Manager.
  - If the Managed Servers are running on VIPs, replace *FINHOST1* and *FINHOST2* with the VIP addresses in [Example 12–1](#).
- 

**Example 12–1 Sample "CostManagementServer" Code**

```
<Location /costManagement>
 SetHandler weblogic-handler
 WebLogicCluster <FINHOST1:port>,<FINHOST2:port>
</Location>
```

3. Repeat Step 2 for all applications.
4. Restart Oracle HTTP Server: cd to *ORACLE\_BASE/config/CommonDomain\_webtier/bin* and enter the following:

```
WEBHOST1> ./opmnctl stopall
WEBHOST1> ./opmnctl startall
```
5. Repeat Steps 1 through 4 on *WEBHOST2*.

## 12.7 Configuring Server Migration for the Managed Servers

Server migration is required for proper failover of Oracle Fusion Financials components in the event of failure in any of the *FINHOST1* and *FINHOST2* nodes. For more information, see [Chapter 18, "Setting Up Server Migration for an Enterprise Deployment."](#)

## 12.8 Validating the System

You should verify URLs to ensure that the appropriate routing and failover are working.

To verify the URLs:

1. Log in to the SCMDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on *FINHOST1* while the Managed Servers on *FINHOST2* are running.
2. Access the following URL to verify that routing and failover are functioning properly. (Ensure the log in prompt is visible.)

- <https://scmexternal.mycompany.com/costManagement/faces/ItemCostProfileWorkarea>
3. Log in to the SCMDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on *FINHOST2*.
  4. Start the Managed Servers on *FINHOST1*.
  5. Repeat Step 2. (Ensure the log in prompt is visible.)
  6. Start all the Managed Servers on *FINHOST2* and verify that they are running on *FINHOST1* and *FINHOST2*.



---

# Scaling Out the Oracle Fusion Projects Domain

This chapter describes how to scale out the Oracle Fusion Projects domain.

This chapter includes the following topics:

- [Section 13.1, "Overview of the Oracle Fusion Projects Domain"](#)
- [Section 13.2, "Prerequisites for Scaling Out the Oracle Fusion Projects Domain"](#)
- [Section 13.3, "Adding a New Machine in the Oracle WebLogic Server Console"](#)
- [Section 13.4, "Packing and Unpacking the Managed Server Domain Home"](#)
- [Section 13.5, "Cloning Managed Servers and Assigning Them to FINHOST2"](#)
- [Section 13.6, "Oracle HTTP Server Configuration"](#)
- [Section 13.7, "Configuring Server Migration for the Managed Servers"](#)
- [Section 13.8, "Validating the System"](#)

## 13.1 Overview of the Oracle Fusion Projects Domain

The Oracle Fusion Projects domain supports the following products:

- Project Foundation
- Project Costing
- Project Billing
- Project Control
- Project Performance Reporting

It integrates with the Oracle Essbase server in the Oracle Business Intelligence domain to support Project Performance Reporting functionality.

[Figure 2–7 in Chapter 2, "Introduction to the Enterprise Deployment Reference Topologies,"](#) shows the topology for the Oracle Fusion Projects domain within the overall reference enterprise deployment topology.

## 13.2 Prerequisites for Scaling Out the Oracle Fusion Projects Domain

Before you begin, ensure the following:

- Node Manager has been started in the Secure Sockets Layer (SSL) mode by following the instructions in [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"](#)

- You are starting with a clean machine if it is the first time it is being used for a scale out
- The `/etc/hosts` file has proper entries. To verify, ping this machine with the fully qualified name of the machine
- The user created on *FINHOST2* should be the same as the user on *FINHOST1*
- The directory structure `/u01/oracle` is mounted to same shared file system as *FINHOST1*
- The directory structure `/u02/local/oracle/config` on *FINHOST2* has been created
- The initial Oracle Fusion Financials deployment on *FINHOST1* has already been done and verified by provisioning

## 13.3 Adding a New Machine in the Oracle WebLogic Server Console

To add a new machine:

1. Log in to the Administration Server:  
`http://prjinternal.mycompany.com:7777/console.`
  2. Navigate to **ProjectsDomain > Environment > Machines.**  
LocalMachine is located in the right-hand pane.
  3. In the left-hand pane, click **Lock & Edit.**
  4. In the right-hand pane, first click **New** to add the remote machine, and then specify the following:
    - Name - enter *FINHOST2*
    - Machine operating system - Unix
  5. Click **Next.**
  6. In the window that opens, set the following attributes:
    - Type - SSL
    - Listen Address - `<FINHOST2>`
- 
- 
- Note:** The "localhost" default value here is wrong.
- 
- 
- Listen port - 5556
7. Click **Finish** and activate the changes.

---

---

**Note:** If you get an error when activating the changes, see [Section 20.8.18, "Administration Console Redirects from Internal URL to Container URL after Activation"](#) for the temporary solution.

---

---

## 13.4 Packing and Unpacking the Managed Server Domain Home

Since the *FINHOST1* domain directory file system is also available from *FINHOST2*, both the `pack` and `unpack` commands can be executed from the *FINHOST2*.

To pack and unpack the Managed Server domain home:

1. Change directory to `ORACLE_BASE/products/fusionapps/oracle_common/common/bin`.
2. Run the pack command:

```
FINHOST2> ./pack.sh -managed=true -domain=ORACLE_BASE/config/domains/
FINHOST1/ProjectsDomain -template=ORACLE_BASE/user_templates/
ProjectsDomain_managed.jar -template_name=
"Projects_Managed_Server_Domain"
```

3. Ensure that `/u02/local/oracle/config/domains/FINHOST2/ProjectsDomain` is empty, and then run the unpack command:

```
FINHOST2> ./unpack.sh -domain=/u02/local/oracle/config/domains/FINHOST2/
ProjectsDomain -template=ORACLE_BASE/user_templates/
ProjectsDomain_managed.jar
```

Here, `ORACLE_BASE` is shared, and `/u02/local` is local to `FINHOST2`.

## 13.5 Cloning Managed Servers and Assigning Them to FINHOST2

To add a Managed Server and assign it to `FINHOST2`:

1. Log in to the Administration Server:  
`http://prjinternal.mycompany.com:7777/console`.
2. Navigate to **ProjectsDomain > Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the *Managed\_Servers* checkbox (for example, **ProjectsFinancialsServer\_1**) and then click **Clone**.
5. Specify the following Server Identity attributes:
  - Server Name - `ProjectsFinancialsServer_2`

---

**Note:** To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to "\_2".

---

- Server Listen Address - `<FINHOST2>`
- Server Listen Port - leave "as is"

---

**Note:** For Oracle SOA Suite server, add a port value that is different than the `soa_server1` server value. This will help in server migration.

---

6. Click **OK**.  
You now should see the newly cloned server, `ProjectsFinancialsServer_2`.
7. Click **ProjectsFinancialsServer\_2** and change the following attributes:
  - Machine - `<FINHOST2>`
  - Cluster Name - accept the default, `ProjectsFinancialsCluster`

---

**Note:** Ensure that this cluster name is the same as the cluster name of the original Managed Server.

---

8. Click **Save** and then **Activate Changes**.
9. Navigate to **ProjectsDomain > Environment > Servers**.
10. From the **Name** column, click the **ProjectsFinancialsServer\_2** scaled-out server link.
11. Click **Lock & Edit**, and then select the **Configuration** tab.
12. Select the **Keystores** tab, and ensure that the keystores value is **Custom Identity and Custom Trust**.
13. Do the following:
  - a. Change the Custom Identity Keystore path to point to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/FINHOST2_fusion_identity.jks` file.
  - b. Leave the Custom Identity Keystore type blank.
  - c. Change the Custom Identity Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - d. Re-enter the Confirm Custom Identity Keystore Passphrase.
  - e. Ensure that the Confirm Custom Trust Keystore path is pointing to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks` file.
  - f. Leave the Custom Trust Keystore type blank.
  - g. Change the Custom Trust Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - h. Re-enter the Custom Trust Keystore Passphrase.
  - i. Click **Save**.
14. Select the **SSL** tab.
  - a. Make sure that Identity and Trust Locations is set to **Keystores**.
  - b. Change the Private Key Alias to `FINHOST2_fusion`.
  - c. Change the Private Key Passphrase to the `keypassword`, as described in the second bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - d. Re-enter the `keypassword` from Step c for the Confirm Private Key Passphrase.
  - e. Click **Save**.
15. Select the **Server Start** tab.

Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

```
-DJDBCProgramName=DS/ProjectsDomain/ProjectsFinancialsServer_2
-Dserver.group=ProjectsFinancialsCluster
```

Click **Save**.

16. Select the **Logging** tab, and then select the **HTTP** tab.

17. Do the following:

- a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.
- b. Change the rotation type to **By Time**.
- c. Leave the **Limit number of retained files** option unchecked.
- d. Leave the **Rotate log file on startup** option unchecked.
- e. Click **Save**.
- f. Expand **Advanced**.
- g. Change the format to **Extended**.
- h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri
sc-status sc(X-ORACLE-DMS-ECID)
cs(ECID-Context) cs(Proxy-Remote-User)
cs(Proxy-Client-IP)
```

- i. Click **Save**.

18. Click **Activate Changes**.

19. Repeat Steps 2 to 18 for all the Managed Servers on this domain.

20. Set the following environment variable on *FINHOST2*:

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/
products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks"
```

21. Stop the domain's Administration Server:

```
FINHOST1> ORACLE_BASE/config/domains/FINHOST1/
ProjectsDomain/bin/stopWebLogic.sh
```

22. Restart the domain's Administration Server:

```
FINHOST2> ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin/wlst.sh

FINHOST2> nmConnect(username='<username>', password='<password>',
domainName='ProjectsDomain', host='FINHOST1',port='5556',
nmType='ssl', domainDir='ORACLE_BASE/config/domains/FINHOST1/ProjectsDomain')

FINHOST2> nmStart('AdminServer')
```

---

**Note:** The *username* and *password* used in the `nmConnect` are the Node Manager credentials (username and password) specified when creating the provisioning response file. This is shown in [Figure 5–3](#) in ["Using the Provisioning Process to Install Components for an Enterprise Deployment"](#).

---

23. Run the newly created Managed Servers:

- a. Log in to the Administration Server:  
`http://prjinternal.mycompany.com:7777/console.`

- b. Navigate to **ProjectsDomain > Environment > Servers > Control**.
- c. Select the newly created Managed Servers and click **Start**.
- d. Navigate to **ProjectsDomain > Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.

## 13.6 Oracle HTTP Server Configuration

To configure Oracle HTTP Server:

1. On *WEBHOST1*:
  - a. Change directory to *ORACLE\_BASE/config/CommonDomain\_webtier/config/OHS/ohs1/moduleconf*.
  - b. Copy *FusionVirtualHost\_prj.conf* to *FusionVirtualHost\_prj.conf.org*.
2. Edit the *FusionVirtualHost\_prj.conf* file, adding the scaled-out host and port to all the WebLogic Application Clusters. Add this to both the Internal and External part of the *FusionVirtualHost\_prj.conf* file. [Example 13–1](#) shows sample code for *ProjectsFinancialsServer*.

---

---

**Notes:**

- Do not add these values for Oracle Enterprise Manager, Oracle WebLogic Server Administration Console, or Oracle Authorization Policy Manager.
  - If the Managed Servers are running on VIPs, replace *FINHOST1* and *FINHOST2* with the VIP addresses in [Example 13–1](#).
- 
- 

### **Example 13–1 Sample "ProjectsFinancialsServer" Code**

```
<Location /projectsFinancials>
 SetHandler weblogic-handler
 WebLogicCluster <FINHOST1:port>,<FINHOST2:port>
</Location>
```

3. Repeat Step 2 for all applications.
4. Restart Oracle HTTP Server: cd to *ORACLE\_BASE/config/CommonDomain\_webtier/bin* and enter the following:

```
WEBHOST1> ./opmnctl stopall
WEBHOST1> ./opmnctl startall
```

5. Repeat Steps 1 through 4 on *WEBHOST2*.

## 13.7 Configuring Server Migration for the Managed Servers

Server migration is required for proper failover of Oracle Fusion Projects components in the event of failure in any of the *FINHOST1* and *FINHOST2* nodes. For more information, see [Chapter 18, "Setting Up Server Migration for an Enterprise Deployment."](#)

## 13.8 Validating the System

You should verify URLs to ensure that the appropriate routing and failover are working.

To verify the URLs:

1. Log in to the `ProjectsDomain` Oracle WebLogic Server Administration Console and stop all the Managed Servers on the `FINHOST1` while the Managed Servers on `FINHOST2` are running.
2. Access the following URLs to verify that routing and failover are functioning properly. (Ensure the log in prompt is visible.)
  - `https://prjexternal.mycompany.com/projectsFinancials/faces/PRJProjectWorkarea`
  - `https://prjexternal.mycompany.com/projectsFinancials/faces/PrjCostWorkArea`
3. Log in to the `ProjectsDomain` Oracle WebLogic Server Administration Console and stop all the Managed Servers on `FINHOST2`.
4. Start the Managed Servers on `FINHOST1`.
5. Repeat Step 2. (Ensure the log in prompt is visible.)
6. Start all the Managed Servers on `FINHOST2` and verify that they are running on `FINHOST1` and `FINHOST2`.



---

# Scaling Out the Oracle Fusion Procurement Domain

This chapter describes how to scale out the Oracle Fusion Projects domain.

This chapter includes the following topics:

- [Section 14.1, "Overview of the Oracle Fusion Procurement Domain"](#)
- [Section 14.2, "Prerequisites for Scaling Out the Oracle Fusion Procurement Domain"](#)
- [Section 14.3, "Adding a New Machine in the Oracle WebLogic Server Console"](#)
- [Section 14.4, "Packing and Unpacking the Managed Server Domain Home"](#)
- [Section 14.5, "Cloning Managed Servers and Assigning Them to FINHOST2"](#)
- [Section 14.6, "Oracle HTTP Server Configuration"](#)
- [Section 14.7, "Configuring Server Migration for the Managed Servers"](#)
- [Section 14.8, "Validating the System"](#)

## 14.1 Overview of the Oracle Fusion Procurement Domain

The Oracle Fusion Procurement domain supports the following products:

- Oracle Fusion Procurement Contracts
- Oracle Fusion Purchasing
- Oracle Fusion Self Service Procurement
- Oracle Fusion Sourcing
- Oracle Fusion Supplier Model
- Oracle Fusion Supplier Portal

Oracle Fusion Procurement integrates with the Oracle Business Intelligence domain for both embedded and PDF reports used by the Procurement and Supplier Portal applications.

[Figure 2–8 in Chapter 2, "Introduction to the Enterprise Deployment Reference Topologies,"](#) shows the topology for the Oracle Fusion Procurement domain within the overall reference enterprise deployment topology.

## 14.2 Prerequisites for Scaling Out the Oracle Fusion Procurement Domain

Before you begin, ensure the following:

- Node Manager has been started in the Secure Sockets Layer (SSL) mode by following the instructions in [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"](#)
- You are starting with a clean machine if it is the first time it is being used for a scale out
- The `/etc/hosts` file has proper entries. To verify, ping this machine with the fully qualified name of the machine
- The user created on `FINHOST2` should be the same as the user on `FINHOST1`
- The directory structure `/u01/oracle` is mounted to same shared file system as `FINHOST1`
- The directory structure `/u02/local/oracle/config` on `FINHOST2` has been created
- The initial Oracle Fusion Financials deployment on `FINHOST1` has already been done and verified by provisioning

## 14.3 Adding a New Machine in the Oracle WebLogic Server Console

To add a new machine:

1. Log in to the Administration Server:  
`http://prcinternal.mycompany.com:7777/console.`
2. Navigate to **ProcurementDomain > Environment > Machines**.  
LocalMachine is located in the right-hand pane.
3. In the left-hand pane, click **Lock & Edit**.
4. In the right-hand pane, first click **New** to add the remote machine, and then specify the following:
  - Name - enter `FINHOST2`
  - Machine operating system - Unix
5. Click **Next**.
6. In the window that opens, set the following attributes:
  - Type - SSL
  - Listen Address - `<FINHOST2>`
7. Click **Finish** and activate the changes.

---

**Note:** The "localhost" default value here is wrong.

---

---

**Note:** If you get an error when activating the changes, see [Section 20.8.18, "Administration Console Redirects from Internal URL to Container URL after Activation"](#) for the temporary solution.

---

## 14.4 Packing and Unpacking the Managed Server Domain Home

Since the *FINHOST1* domain directory file system is also available from *FINHOST2*, both the pack and unpack commands can be executed from the *FINHOST2*.

To pack and unpack the Managed Server domain home:

1. Change directory to *ORACLE\_BASE*/products/fusionapps/oracle\_common/common/bin.
2. Run the pack command:
 

```
FINHOST2> ./pack.sh -managed=true -domain=ORACLE_BASE/config/domains/
FINHOST1/ProcurementDomain -template=ORACLE_BASE/user_templates/
ProcurementDomain_managed.jar -template_name=
"Procurement_Managed_Server_Domain"
```
3. Ensure that */u02/local/oracle/config/domains/FINHOST2/ProcurementDomain* is empty, and then run the unpack command:
 

```
FINHOST2> ./unpack.sh -domain=/u02/local/oracle/config/domains/FINHOST2/
ProcurementDomain -template=ORACLE_BASE/user_templates/
ProcurementDomain_managed.jar
```

Here, *ORACLE\_BASE* is shared, and */u02/local* is local to *FINHOST2*.

## 14.5 Cloning Managed Servers and Assigning Them to FINHOST2

To add a Managed Server and assign it to *FINHOST2*:

1. Log in to the Administration Server:  
`http://prcinternal.mycompany.com:7777/console.`
2. Navigate to **ProcurementDomain > Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the *Managed\_Servers* checkbox (for example, **ProcurementServer\_1**) and then click **Clone**.
5. Specify the following Server Identity attributes:
  - Server Name - *ProcurementServer\_2*

---

**Note:** To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to "\_2".

---

- Server Listen Address - *<FINHOST2>*
- Server Listen Port - leave "as is"

---

**Note:** For Oracle SOA Suite server, add a port value that is different than the *soa\_server1* server value. This will help in server migration.

---

6. Click **OK**.  
You now should see the newly cloned server, *ProcurementServer\_2*.
7. Click **ProcurementServer\_2** and change the following attributes:

- Machine - `<FINHOST2>`
- Cluster Name - accept the default, `ProcurementCluster`

---

**Note:** Ensure that this cluster name is the same as the cluster name of the original Managed Server.

---

8. Click **Save** and then **Activate Changes**.
9. Navigate to **ProcurementDomain > Environment > Servers**.
10. From the **Name** column, click the **ProcurementServer\_2** scaled-out server link.
11. Click **Lock & Edit**, and then select the **Configuration** tab.
12. Select the **Keystores** tab, and ensure that the keystores value is **Custom Identity and Custom Trust**.
13. Do the following:
  - a. Change the Custom Identity Keystore path to point to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/FINHOST2_fusion_identity.jks` file.
  - b. Leave the Custom Identity Keystore type blank.
  - c. Change the Custom Identity Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - d. Re-enter the Confirm Custom Identity Keystore Passphrase.
  - e. Ensure that the Confirm Custom Trust Keystore path is pointing to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks` file.
  - f. Leave the Custom Trust Keystore type blank.
  - g. Change the Custom Trust Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - h. Re-enter the Custom Trust Keystore Passphrase.
  - i. Click **Save**.
14. Select the **SSL** tab.
  - a. Make sure that Identity and Trust Locations is set to **Keystores**.
  - b. Change the Private Key Alias to `FINHOST2_fusion`.
  - c. Change the Private Key Passphrase to the `keypassword`, as described in the second bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - d. Re-enter the `keypassword` from Step c for the Confirm Private Key Passphrase.
  - e. Click **Save**.
15. Select the **Server Start** tab.

Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

```
-DJDBCProgramName=DS/ProcurementDomain/ProcurementServer_2
-Dserver.group=ProcurementCluster
```

Click **Save**.

16. Select the **Logging** tab, and then select the **HTTP** tab.

17. Do the following:

- a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.
- b. Change the rotation type to **By Time**.
- c. Leave the **Limit number of retained files** option unchecked.
- d. Leave the **Rotate log file on startup** option unchecked.
- e. Click **Save**.
- f. Expand **Advanced**.
- g. Change the format to **Extended**.
- h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri
sc-status sc(X-ORACLE-DMS-ECID)
cs(ECID-Context) cs(Proxy-Remote-User)
cs(Proxy-Client-IP)
```

- i. Click **Save**.

18. Click **Activate Changes**.

19. Repeat Steps 2 to 18 for all the Managed Servers on this domain.

20. Set the following environment variable on *FINHOST2*:

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/
products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks"
```

21. Stop the domain's Administration Server:

```
FINHOST1> ORACLE_BASE/config/domains/FINHOST1/
ProcurementDomain/bin/stopWebLogic.sh
```

22. Restart the domain's Administration Server:

```
FINHOST2> ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin/wlst.sh

FINHOST2> nmConnect(username='<username>', password='<password>',
domainName='ProcurementDomain', host='FINHOST1',port='5556',
nmType='ssl', domainDir='ORACLE_
BASE/config/domains/FINHOST1/ProcurementDomain')

FINHOST2> nmStart('AdminServer')
```

---

**Note:** The *username* and *password* used in the `nmConnect` are the Node Manager credentials (username and password) specified when creating the provisioning response file. This is shown in [Figure 5–3](#) in "Using the Provisioning Process to Install Components for an Enterprise Deployment".

---

23. Run the newly created Managed Servers:

- a. Log in to the Administration Server:  
`http://prcinternal.mycompany.com:7777/console`.
- b. Navigate to **ProcurementDomain > Environment > Servers > Control**.
- c. Select the newly created Managed Servers and click **Start**.
- d. Navigate to **ProcurementDomain > Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.

## 14.6 Oracle HTTP Server Configuration

To configure Oracle HTTP Server:

1. On *WEBHOST1*:
  - a. Change directory to `ORACLE_BASE/config/CommonDomain_webtier/config/OHS/ohs1/moduleconf`.
  - b. Copy `FusionVirtualHost_prc.conf` to `FusionVirtualHost_prc.conf.org`.
2. Edit the `FusionVirtualHost_prc.conf` file, adding the scaled-out host and port to all the WebLogic Application Clusters. Add this to both the Internal and External part of the `FusionVirtualHost_prc.conf` file. [Example 14–1](#) shows sample code for `ProcurementServer`.

---

---

**Notes:**

- Do not add these values for Oracle Enterprise Manager, Oracle WebLogic Server Administration Console, or Oracle Authorization Policy Manager.
  - If the Managed Servers are running on VIPs, replace *FINHOST1* and *FINHOST2* with the VIP addresses in [Example 14–1](#).
- 
- 

### **Example 14–1 Sample "ProcurementServer" Code**

```
<Location /procurement>
 SetHandler weblogic-handler
 WebLogicCluster <FINHOST1:port>,<FINHOST2:port>
</Location>
```

3. Repeat Step 2 for all applications.
4. Restart Oracle HTTP Server: `cd` to `ORACLE_BASE/config/CommonDomain_webtier/bin` and enter the following:  

```
WEBHOST1> ./opmnctl stopall
WEBHOST1> ./opmnctl startall
```
5. Repeat Steps 1 through 4 on *WEBHOST2*.

## 14.7 Configuring Server Migration for the Managed Servers

Server migration is required for proper failover of Oracle Fusion Procurement components in the event of failure in any of the *FINHOST1* and *FINHOST2* nodes. For more information, see [Chapter 18, "Setting Up Server Migration for an Enterprise Deployment."](#)

## 14.8 Validating the System

You should verify URLs to ensure that the appropriate routing and failover are working.

To verify the URLs:

1. Log in to the `ProcurementDomain` Oracle WebLogic Server Administration Console and stop all the Managed Servers on the `FINHOST1` while the Managed Servers on `FINHOST2` are running.
2. Access the following URLs to verify that routing and failover are functioning properly. (Ensure the log in prompt is visible.)
  - `https://prcexternal.mycompany.com/procurement/faces/PrcPoPurchasingWorkarea`
  - `https://prcexternal.mycompany.com/supplierPortal/faces/PrcPosSupplierPortalWorkarea`
3. Log in to the `ProcurementDomain` Oracle WebLogic Server Administration Console and stop all the Managed Servers on `FINHOST2`.
4. Start the Managed Servers on `FINHOST1`.
5. Repeat Step 2. (Ensure the log in prompt is visible.)
6. Start all the Managed Servers on `FINHOST2` and verify that they are running on `FINHOST1` and `FINHOST2`.



---

# Scaling Out the Oracle Business Intelligence Domain

This chapter describes how to scale out the Oracle Business Intelligence domain.

This chapter includes the following topics:

- [Section 15.1, "Overview of the Oracle Business Intelligence Domain"](#)
- [Section 15.2, "Prerequisites for Scaling Out the Oracle Business Intelligence Domain"](#)
- [Section 15.3, "Starting the Default Node Manager"](#)
- [Section 15.4, "Prerequisites for Scaling Out Oracle Business Intelligence on FINHOST2"](#)
- [Section 15.5, "Scaling Out Oracle Business Intelligence Components"](#)
- [Section 15.6, "Configuring Oracle Essbase Clustering"](#)
- [Section 15.7, "Validating the System"](#)

## 15.1 Overview of the Oracle Business Intelligence Domain

Oracle Fusion Financials uses Oracle Business Intelligence Foundation's common set of Oracle Business Intelligence tools and shared services that enable the Enterprise Performance Management system.

Oracle Fusion Financials uses the following Oracle Business Intelligence tools for financial reporting and analysis purposes:

- Oracle Essbase
- Oracle Business Intelligence Publisher (Oracle BI Publisher)
- Oracle Transaction Business Intelligence
- Oracle Business Intelligence Analytics

### Oracle Essbase

Oracle Fusion General Ledger combines the traditional general ledger functionality with Oracle Essbase functionality, which is seamlessly embedded within the Oracle Fusion General Ledger. At the time users create their chart of accounts, the balances cube is created automatically. Later, if you make a change such as a cost center is added or a date effective hierarchy is modified, the General Ledger automatically creates or modifies the corresponding balances cube hierarchy. As transactions or journals are posted, the General Ledger automatically updates the multidimensional

cube. Unlike a data warehouse, no batch programs need to be run to populate the balances cube; it is all happening in real time when a journal is posted.

### **Oracle Business Intelligence Publisher**

Oracle BI Publisher provides the ability to create and format high quality reports across Oracle Fusion Financials applications. It applies templates, which users design in familiar desktop tools, to standard extracts and reports. For example, it is used widely in Oracle Fusion Payments for formatting of the check payments and electronic payment files.

### **Oracle Transaction Business Intelligence**

Oracle Transaction Business Intelligence is widely used in Oracle Fusion Financials as a reporting tool. Using Oracle Transaction Business Intelligence, users can perform adhoc queries directly from transaction tables using drag-and-drop functionality to build custom reports in real time from the various Oracle Fusion Financials applications. It helps immensely in reducing the need to build and maintain customized reports.

### **Oracle Business Intelligence Analytics**

Oracle Business Intelligence Analytics provides day-to-day key performance indicators (KPIs) of any item in Oracle Fusion Financials. Intelligence and analytics are embedded within the context of business transactions to help users complete the transactions. For example, before users post a journal, the system will tell them the impact the journal will have on the account balances. This eliminates the need to navigate to a separate page to run a query or run a report. End users will not be distracted from the task at hand, reporting and process demand is reduced, and smarter decisions are made in the context of the transaction.

Figure 2–10 in Chapter 2, "Introduction to the Enterprise Deployment Reference Topologies," shows the topology for the Oracle Business Intelligence domain within the overall reference enterprise deployment topology.

## **15.2 Prerequisites for Scaling Out the Oracle Business Intelligence Domain**

Before you begin, ensure the following:

- Node Manager has been started in the Secure Sockets Layer (SSL) mode by following the instructions in [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"](#)
- You are starting with a clean machine if it is the first time it is being used for a scale out
- The `/etc/hosts` file has proper entries. To verify, ping this machine with the fully qualified name of the machine
- The user created on `FINHOST2` should be the same as the user on `FINHOST1`
- The directory structure `/u01/oracle` is mounted to same shared file system as `FINHOST1`
- The directory structure `/u02/local/oracle/config` on `FINHOST2` has been created
- The initial Oracle Fusion Financials deployment on `FINHOST1` has already been done and verified by provisioning

- The Administration Console's **Follow Configuration Changes** feature has been disabled (to eliminate redirections):
  1. Log into the Administration Console (<http://biinternal.mycompany.com:7777/console>) and go to **Preferences > Shared Preferences**.
  2. Deselect **Follow Configuration Changes** and click **Save**.

## 15.3 Starting the Default Node Manager

To start the default Node Manager:

1. Stop any Node Manager running on *FINHOST2* using one of the following methods:
  - Use Ctrl+C in the shell where it was started
  - Use the standard process-identification and kill commands in the operating system appropriate to Oracle Fusion Financials and the Oracle Fusion Applications enterprise deployment.
2. Change directory to *ORACLE\_BASE/products/fusionapps/wlserver\_10.3/common/nodemanager* and edit the *nodemanager.properties* file with the following:

```
SecureListener=false
```
3. Change directory to *ORACLE\_BASE/products/fusionapps/oracle\_common/common/bin* and run the following script:

```
./setNMProps.sh
```
4. Change directory to *ORACLE\_BASE/products/fusionapps/wlserver\_10.3/server/bin* and run the following script:

```
./startNodeManager.sh
```

Node Manager starts on *FINHOST2*.

---

---

**Note:** Steps 2 through 4 will enable Node Manager on *FINHOST2* and the Administrator Console to communicate on Plain Socket.

---

---

## 15.4 Prerequisites for Scaling Out Oracle Business Intelligence on FINHOST2

Prerequisites include the following:

- [Configuring JMS for Oracle BI Publisher](#)
- [Setting the Listen Address for bi\\_server1 Managed Server](#)
- [Updating the FusionVirtualHost\\_bi.conf Configuration File](#)

### 15.4.1 Configuring JMS for Oracle BI Publisher

You must configure the location for all persistence stores to a directory visible from both nodes. Change all persistent stores to use this shared base directory.

1. Log in to the Administration Console  
(<http://biinternal.mycompany.com:7777/console>).
2. In the Domain Structure window, expand the **Services** node and then click the **Persistent Stores** node. The Summary of Persistent Stores page is displayed.
3. In the Change Center, click **Lock & Edit**.
4. Click **BipJmsStore** and enter a directory that is located in the shared storage. This shared storage is accessible from both *FINHOST1* and *FINHOST2*:  
`ORACLE_BASE/config/domains/FINHOST1/BIDomain/BipJmsStore`
5. Click **Save** and then click **Activate Changes**.  
The changes will not take effect until the Managed Server is restarted.
6. Do the following:
  - a. Ensure that Node Manager is up and running.
  - b. On the Summary of Servers page, select the **Control** tab.
  - c. Select **bi\_server1** in the table and then click **Shutdown**.
  - d. After the server has shut down, select **bi\_server1** in the table and then click **Start**.
7. Run the following commands to restart the Oracle Business Intelligence system components:

```
$ cd /u02/local/oracle/config/BIInstance/bin
$./opmnctl stopall
$./opmnctl startall
```

## 15.4.2 Setting the Listen Address for bi\_server1 Managed Server

Make sure that you have performed the steps described in [Section 16.1, "Enabling Virtual IPs on FINHOST1 and FINHOST2"](#) before setting the **bi\_server1** listen address.

To set the listen address for the Managed Server:

1. Log in to the Administration Console  
(<http://biinternal.mycompany.com:7777/console>).
2. In the Change Center, click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select **bi\_server1** in the table. The Settings page for **bi\_server1** is displayed.
6. Set the **Listen Address** to *BIVH1*.
7. Click **Save**.
8. Click **Activate Changes**.
9. The changes will not take effect until the **bi\_server1** Managed Server is restarted (ensure that Node Manager is up and running):
  - a. On the Summary of Servers page, select the **Control** tab.
  - b. Select **bi\_server1** in the table and then click **Shutdown**.

- c. After the server has shut down, select **bi\_server1** in the table and then click **Start**.

10. Restart the Oracle Business Intelligence system components, as follows:

```
$ cd /u02/local/oracle/config/BIInstance/bin
$./opmnctl stopall
$./opmnctl startll
```

### 15.4.3 Updating the FusionVirtualHost\_bi.conf Configuration File

To enable Oracle HTTP Server to route to `bi_cluster`, which contains the `bi_servern` Managed Servers, you must set the `WebLogicCluster` parameter to the list of nodes in the cluster:

1. On `WEBHOST1` and `WEBHOST2`, update the `WebLogicCluster` parameter in the `ORACLE_BASE/config/CommonDomain_webtiern/config/OHS/ohs1/moduleconf/FusionVirtualHost_bi.conf` file to contain a cluster list of virtual host:port entries.

---

**Note:** You must update the `FusionVirtualHost_bi.conf` file in two locations:

- Under the internal virtual host for Oracle Business Intelligence
  - Under the external virtual host for Oracle Business Intelligence
- 

For example, for the internal virtual host:

```
<LocationMatch ^/analytics/>
SetHandler weblogic-handler
WebLogicCluster BIVH1:10217,BIVH2:10217
</LocationMatch>
```

For the external virtual host:

```
<LocationMatch ^/analytics/>
SetHandler weblogic-handler
WebLogicCluster BIVH1:10217,BIVH2:10217
WLProxySSL ON
WLProxySSLPassThrough ON
RewriteEngine ON
RewriteOptions inherit
</LocationMatch>
```

2. On `WEBHOST1` and `WEBOST2`, add the following context roots to the `ORACLE_BASE/config/CommonDomain_webtiern/config/OHS/ohs1/moduleconf/FusionVirtualHost_bi.conf` file:

**Example 15–1 # Internal Virtual Host Section**

```
RedirectMatch 301 ^/bioofficeclient$ /bioofficeclient/

RedirectMatch 301 ^/bimiddleware$ /bimiddleware/

RedirectMatch 301 ^/rtis$ /rtis/

RedirectMatch 301 ^/bisearch$ /bisearch/

<LocationMatch ^/bioofficeclient/>
```

```
SetHandler weblogic-handler
WebLogicCluster BIVH1:10217,BIVH2:10217
</LocationMatch>

<LocationMatch ^/bimiddleware/>
SetHandler weblogic-handler
WebLogicCluster BIVH1:10217,BIVH2:10217
</LocationMatch>

<LocationMatch ^/rtis/>
SetHandler weblogic-handler
WebLogicCluster BIVH1:10217,BIVH2:10217
</LocationMatch>

<LocationMatch ^/bisearch/>
SetHandler weblogic-handler
WebLogicCluster BIVH1:10217,BIVH2:10217
</LocationMatch>
```

**Example 15–2 # External Virtual Host Section**

```
RedirectMatch 301 ^/bioofficeclient$ /bioofficeclient/

RedirectMatch 301 ^/bimiddleware$ /bimiddleware/

RedirectMatch 301 ^/rtis$ /rtis/

RedirectMatch 301 ^/bisearch$ /bisearch/

<LocationMatch ^/bioofficeclient/>
SetHandler weblogic-handler
WebLogicCluster BIVH1:10217,BIVH2:10217
WLProxySSL ON
WLProxySSLPassThrough ON
RewriteEngine ON
RewriteOptions inherit
</LocationMatch>

<LocationMatch ^/bimiddleware/>
SetHandler weblogic-handler
WebLogicCluster BIVH1:10217,BIVH2:10217
WLProxySSL ON
WLProxySSLPassThrough ON
RewriteEngine ON
RewriteOptions inherit
</LocationMatch>

<LocationMatch ^/rtis/>
SetHandler weblogic-handler
WebLogicCluster BIVH1:10217,BIVH2:10217
WLProxySSL ON
WLProxySSLPassThrough ON
RewriteEngine ON
RewriteOptions inherit
</LocationMatch>

<LocationMatch ^/bisearch/>
SetHandler weblogic-handler
WebLogicCluster BIVH1:10217,BIVH2:10217
```

```

WLProxySSL ON
WLProxySSLPassThrough ON
RewriteEngine ON
RewriteOptions inherit
</LocationMatch>

```

**3. Restart Oracle HTTP Server on both *WEBHOST1* and *WEBHOST2*, as follows:**

```

WEBHOST1> ORACLE_BASE/config/CommonDomain_webtier/bin/opmnctl restartproc
ias-component=ohs1
WEBHOST2> ORACLE_BASE/config/CommonDomain_webtier1/bin/opmnctl restartproc
ias-component=ohs1

```

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

Sample scenarios include:

- **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 dynamically at run time.
- **Example 2:** You have a three-node cluster, but only two nodes are listed in the configuration. However, if both listed nodes are down when you start Oracle HTTP Server, then the plug-in would fail to route to the cluster. You must ensure that at least one of the listed nodes is running when you start Oracle HTTP Server.

If you list all the members of the cluster, then you guarantee you can route to the cluster, assuming at least one member is running when Oracle HTTP Server is started. For more information on configuring the WebLogic Server plug-in, see *Oracle Fusion Middleware Using Web Server Plug-Ins with Oracle WebLogic Server*.

## 15.5 Scaling Out Oracle Business Intelligence Components

This section describes how to scale out the Oracle Business Intelligence system using the Configuration Assistant. It is assumed that an Oracle Business Intelligence *ORACLE\_BASE* (binaries) has already been installed and is available from *FINHOST1* and *FINHOST2*, and that a domain with an Administration Server has been created. This is the domain that will be extended in this chapter to support Oracle Business Intelligence components.

---

**Important:** Oracle strongly recommends that you read the Oracle Fusion Middleware release notes for any additional installation and deployment considerations before starting the setup process.

---

This section includes the following topics:

- [Section 15.5.1, "Scaling Out the Oracle Business Intelligence System on \*FINHOST2\*"](#)
- [Section 15.5.2, "Starting Node Manager in SSL Mode"](#)
- [Section 15.5.3, "Scaling Out the System Components"](#)

- [Section 15.5.4, "Configuring Secondary Instances of Singleton System Components"](#)
- [Section 15.5.5, "Configuring the bi\\_server2 Managed Server"](#)
- [Section 15.5.6, "Performing Additional Configuration for Oracle Business Intelligence High Availability"](#)
- [Section 15.5.7, "Configuring a Default Persistence Store for Transaction Recovery"](#)
- [Section 15.5.8, "Starting and Validating Oracle Business Intelligence on FINHOST2"](#)
- [Section 15.5.9, "Validating Access Through Oracle HTTP Server"](#)
- [Section 15.5.10, "Configuring Node Manager for the Managed Servers"](#)
- [Section 15.5.11, "Configuring Server Migration for the Managed Servers"](#)

## 15.5.1 Scaling Out the Oracle Business Intelligence System on FINHOST2

To scale out the Oracle Business Intelligence system:

1. Ensure that the `bi_server1` server is running.
2. In the `ORACLE_BASE/products/fusionapps/registry.xml` file, change

```
<component name="WebLogic Server" version="10.3.6.0"
InstallDir="ORACLE_BASE/products/fusionapps/wlserver_10.3">
```

to

```
<component name="WebLogic Server" version="Temporary"
InstallDir="ORACLE_BASE/products/fusionapps/wlserver_10.3">
```
3. Change directory to the location of the Configuration Assistant:

```
FINHOST2> ORACLE_BASE/products/fusionapps/bi/bin
```
4. Start the Oracle Business Intelligence Configuration Assistant:

```
FINHOST2> ./config.sh
```
5. In the Welcome screen, click **Next**.
6. In the Prerequisite Checks screen, verify that all checks complete successfully, and then click **Next**.
7. In the Create or Scale out BI System screen, select **Scale Out BI System** and enter the following:
  - **Host Name:** `FINHOST1`
  - **Port:** `10201`
  - **User name:** `WLS_Administrator`
  - **User Password:** `WLS_Administrator_password`Click **Next**.
8. In the Scale Out BI System Details screen, enter the following:
  - **Middleware Home:** `ORACLE_BASE /products/fusionapps` (dimmed)

- **Oracle Home:** *ORACLE\_BASE*/products/fusionapps/bi (dimmed)
- **WebLogic Server Home:** *ORACLE\_BASE*/products/fusionapps/wlserver\_10.3 (dimmed)
- **Domain Home:** /u02/local/oracle/config/domains/*FINHOST1* /BIDomain
- **Applications Home:**  
/u02/local/oracle/config/applications/*FINHOST1*/BIDomain
- **Instance Home:** Defaults to /u02/local/oracle/config/BIInstance1
- **Instance Name:** BIInstance1 (dimmed)

Click **Next**.

9. In the Configure Ports screen, select "Specify Ports using Configuration File."

Use the *bi\_staticports.ini* file from the *ORACLE\_BASE*/products/ports directory.

Click **Next**.

10. In the Specify Security Updates screen, choose whether you want to receive security updates from Oracle support and if you do, enter your e-mail address.

Click **Next**.

11. In the Summary screen, click **Configure**.

12. In the Configuration Progress screen, verify that all the Configuration Tools have completed successfully and click **Next**.

13. In the Complete screen, click **Finish**.

## 15.5.2 Starting Node Manager in SSL Mode

To start Node Manager in SSL mode:

1. Stop the default Node Manager running on *FINHOST2* using one of the following methods:

- Use CTRL+C in the shell where it was started
- Use the standard process-identification and kill commands in the operating system appropriate to Oracle Fusion Financials and the Oracle Fusion Applications enterprise deployment.

2. Start Node Manager in SSL mode on *FINHOST2*:

```
FINHOST2> cd ORACLE_BASE/products/fusionapps/wlserver_10.3/common/nodemanager/FINHOST2
```

```
FINHOST2> ./startNodeManagerWrapper.sh
```

3. Update the Node Manager for the *FINHOST2* machine using the Oracle WebLogic Server Console by doing the following:

- a. Log in to the Administration Server:  
<http://biinternal.mycompany.com:7777/console>.
- b. Navigate to **BIDomain > Environment > Machines**.
- c. In the left-hand pane, click **Lock & Edit**.
- d. In the right-hand pane, click *FINHOST2*.

- e. In the window that opens, click the **Node Manager** tab and set the following attributes:
  - Type - SSL
  - Listen Address - <FINHOST2>
  - Listen Port - 5556
4. Click **Save** and then **Activate Changes**.  
The changes will not take effect until the bi\_server2 Managed Server is restarted.
5. Do the following:
  - a. Stop the Administration Server:
 

```
FINHOST1> ORACLE_BASE/config/domains/FINHOST1/BIDomain/bin/stopWebLogic.sh
```
  - b. Connect to the Administration Server through nmConnect and start the Administration Server using nmstart:
    - Set the following environment variable:
 

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks"
```
    - Start the Administration Server:
 

```
FINHOST1> cd ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin
 FINHOST1> ./wlst.sh
```
    - In the WLST shell, execute the following command:
 

```
wls:/offline> nmConnect (username='Admin_User',password='Admin_Password',host='FINHOST1',port='5556', nmType='ssl', domainDir='ORACLE_BASE/config/domains/FINHOST1/BIDomain')
 wls:/nm/domain_name> nmStart ('AdminServer')
```

---

**Note:** The username and password used in the nmConnect are the Node Manager credentials (username and password) specified when creating the provisioning response file. This is shown in [Figure 5–3 in Chapter 5, "Using the Provisioning Process to Install Components for an Enterprise Deployment."](#)

---

- c. Restart the bi\_server2 Managed Server:
  - On the Summary of Servers page, select the **Control** tab.
  - Select **bi\_server2** in the table and then click **Shutdown**.
  - After the server has shut down, select **bi\_server2** in the table and then click **Start**.

### 15.5.3 Scaling Out the System Components

To scale out the system components, do the following in Oracle Enterprise Manager Fusion Middleware Control:

1. Log in to Fusion Middleware Control  
(<http://biinternal.mycompany.com:7777/em>).
2. Expand the **Business Intelligence** node in the Farm\_BIDomain window.

3. Click **coreapplication**.
4. Click **Capacity Management**, then click **Scalability**.
5. Click **Lock and Edit Configuration**.
6. For the *FINHOST2* BIInstance1 Oracle instance, increment the Oracle Business Intelligence components by 1:
  - BI Servers
  - Presentation Servers
  - JavaHosts
7. Change the **Port Range From** and **Port Range To** to be the same as the *FINHOST1* BIInstance Oracle instance.
8. Click **Apply**.
9. Click **Activate Changes**.

You do not need to restart at this point, because you will perform a restart after completing the steps in [Section 15.5.4, "Configuring Secondary Instances of Singleton System Components."](#)

## 15.5.4 Configuring Secondary Instances of Singleton System Components

Oracle Business Intelligence Scheduler and Oracle Business Intelligence Cluster Controller are singleton components that operate in active/passive mode. Configure a secondary instance of these components so that they are distributed for high availability.

To configure secondary instances, do the following in Fusion Middleware Control:

1. Log in to Fusion Middleware Control  
(<http://biinternal.mycompany.com:7777/em>).
2. Expand the **Business Intelligence** node in the Farm\_BIDomain window.
3. Click **coreapplication**.
4. Click **Availability**, then click **Failover**.
5. Click **Lock and Edit Configuration** to activate the Primary/Secondary Configuration section of the Availability tab.
6. Specify the Secondary Host/Instance for BI Scheduler and BI Cluster Controller.
7. Click **Apply**.  
Under Potential Single Points of Failure, no problem should be reported for BI Scheduler and BI Cluster Controller.
8. Click **Activate Changes**.
9. Click **Restart to apply recent changes**.
10. From **Manage System**, click **Restart**.
11. Click **Yes** when prompted to confirm that you want to restart all Business Intelligence components.

## 15.5.5 Configuring the bi\_server2 Managed Server

This section explains how to configure the bi\_server2 Managed Server, and contains the following topics:

- [Section 15.5.5.1, "Setting the Listen Address for the bi\\_server2 Managed Server"](#)
- [Section 15.5.5.2, "Configuring Custom Identity and Custom Trust for the bi\\_server2 Managed Server"](#)
- [Section 15.5.5.3, "Disabling Host Name Verification for the bi\\_server2 Managed Server"](#)
- [Section 15.5.5.4, "Adding bi\\_server2 System Properties to the Server Start Tab"](#)

#### 15.5.5.1 Setting the Listen Address for the bi\_server2 Managed Server

Make sure that you have performed the steps described in [Section 16.1, "Enabling Virtual IPs on FINHOST1 and FINHOST2"](#) before setting the bi\_server2 listen address.

To set the listen address for the Managed Server:

1. Log in to the Oracle WebLogic Server Administration Console (<http://biinternal.mycompany.com:7777/console>).
2. In the Change Center, click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select **bi\_server2** in the table. The settings page for bi\_server2 is displayed.
6. Set the **Listen Address** to *BIVH2*.
7. Click **Save**.
8. Click **Activate Changes**.

The changes will not take effect until the Managed Server is restarted.

9. Do the following:
  - a. Ensure that Node Manager is up and running.
  - b. On the Summary of Servers page, select the **Control** tab.
  - c. Select **bi\_server2** in the table and then click **Shutdown**.
  - d. After the server has shut down, select **bi\_server2** in the table and then click **Start**.

#### 15.5.5.2 Configuring Custom Identity and Custom Trust for the bi\_server2 Managed Server

To configure custom identity and custom trust:

1. Log in to the Oracle WebLogic Server Administration Console (<http://biinternal.mycompany.com:7777/console>).
2. In the Change Center, click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**.

The Summary of Servers page displays.
5. Select **bi\_server2** in the table. The Settings page for bi\_server2 displays.
6. Click **Keystores**, and then do the following:
  - a. Click **Change** next to **Demo Identity and Demo Trust**.

- b. Select **Custom Identity** and **Custom Trust** from the **Keystores** dropdown list and click **Save**.
  - c. Under **Identity**, do the following:
    - Change the Custom Identity Keystore entry to point to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/FINHOST2_fusion_identity.jks` file.
    - Enter and confirm the Custom Identity Keystore Passphrase. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
  - d. Under **Trust**, do the following:
    - Change the Custom Identity Keystore entry to point to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks` file.
    - Enter and confirm the Custom Trust Keystore Passphrase. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
    - Click **Save**.
7. Click **SSL**, and then do the following:
  - a. Ensure that Identity and Trust Locations is set to **Keystores**.
  - b. Under **Identity**, do the following:
    - Change the Private Key Alias to `FINHOST2_fusion`.
    - Enter and confirm the Private Key Passphrase to the `keypassword`, as described in the second bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
    - Click **Save**.
8. Click **Activate Changes**.
9. Set the following property in `ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin/wlst.sh`:
 

```
WLST_PROPERTIES="-Dweblogic.wlstHome='${WLST_HOME}'
-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/
products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks ${WLST_
PROPERTIES}"
```

### 15.5.5.3 Disabling Host Name Verification for the bi\_server2 Managed Server

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server (see [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"](#)). If you have not configured the server certificates, you will receive errors when managing the different WebLogic servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again once the enterprise deployment topology configuration is complete as described in [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment."](#)

To disable host name verification:

1. Log in to Oracle WebLogic Server Administration Console (<http://biinternal.mycompany.com:7777/console>).

2. Click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select **bi\_server2** in the table. The settings page for the server is displayed.
6. Click the **SSL** tab.
7. Expand the **Advanced** section of the page.
8. Set **Host Name Verification** to **None**.
9. Click **Save**.
10. Click **Activate Changes**.
11. The change will not take effect until the **bi\_server2** Managed Server is restarted (make sure that Node Manager is up and running):
  - a. In the Summary of Servers screen, select the **Control** tab.
  - b. Select **bi\_server2** in the table and then click **Shutdown**.
  - c. Restart **bi\_server2**.
12. Restart the Oracle Business Intelligence system components:

```
$ cd /u02/local/oracle/config/BIIInstance1/bin
$./opmnctl stopall
$./opmnctl startall
```

#### 15.5.5.4 Adding bi\_server2 System Properties to the Server Start Tab

After scaling out the **bi\_server2** Managed Server, you must add a new system property to the **Server Start** tab of this Managed Server.

1. Log in to the Oracle WebLogic Server Administration Console (<http://biinternal.mycompany.com:7777/console>).
2. Click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**.

The Summary of Servers page displays.
5. Select **bi\_server2** in the table.

The settings page for the server displays.
6. Click **Server Start**.
7. Add the following property to the arguments:

```
-DJDBCProgramName=DS/BIDomain/bi_server2
```
8. Click **Save** and then **Activate Changes**.
9. Restart the **bi\_server2** Managed Server (ensure sure that Node Manager is up and running):
  - a. In the Summary of Servers screen, select the **Control** tab.
  - b. Select **bi\_server2** in the table and then click **Shutdown**.
  - c. Restart **bi\_server2**.
10. Restart the BI System Components:

```
$ cd /u02/local/oracle/config/BIInstance1/bin
$./opmnctl stopall
$./opmnctl startall
```

## 15.5.6 Performing Additional Configuration for Oracle Business Intelligence High Availability

This section describes additional high availability configuration tasks for Oracle BI Enterprise Edition, Oracle Real-Time Decisions, Oracle BI Publisher, and Oracle Financial Reports. It includes the following topics:

- [Section 15.5.6.1, "Additional Configuration Tasks for Oracle BI Scheduler"](#)
- [Section 15.5.6.2, "Additional Configuration Tasks for Oracle Real-Time Decisions"](#)
- [Section 15.5.6.3, "Additional Configuration Tasks for Oracle BI Publisher"](#)
- [Section 15.5.6.4, "Additional Configuration Tasks for Oracle BI for Microsoft Office"](#)
- [Section 15.5.6.5, "Additional Configuration Tasks for Oracle Financial Reporting"](#)

### 15.5.6.1 Additional Configuration Tasks for Oracle BI Scheduler

If you use server-side scripts with Oracle BI Scheduler, it is recommended that you configure a shared directory for the scripts so that they can be shared by all Oracle BI Scheduler components in a cluster.

Perform these steps only if you are using server-side scripts.

To share Oracle BI Scheduler scripts:

1. Create an *ORACLE\_BASE*/config/BIShared/OracleBISchedulerComponent/coreapplication\_obisch1 directory.
2. From *FINHOST1*, copy the default Oracle BI Scheduler scripts (for example, /u02/local/oracle/config/BIInstance/bifoundation/OracleBISchedulerComponent/coreapplication\_obisch1/scripts/common) and custom Oracle BI Scheduler scripts (for example, /u02/local/oracle/config/BIInstance/bifoundation/OracleBISchedulerComponent/coreapplication\_obisch1/scripts/scheduler) to the following location:  
*ORACLE\_BASE*/config/BIShared/OracleBISchedulerComponent/coreapplication\_obisch1
3. Update the SchedulerScriptPath and DefaultScriptPath elements of the Oracle BI Scheduler instanceconfig.xml file, as follows:
  - SchedulerScriptPath: Refers to the path where Oracle BI Scheduler-created job scripts are stored. Change this to the path of the shared BI Scheduler scripts location.
  - DefaultScriptPath: Specifies the path where user-created job scripts (not agents) are stored. Change this to the path of the shared BI Scheduler scripts location.

The instanceconfig.xml files for Oracle BI Scheduler are in the following locations:

**On *FINHOST1*:**

```
/u02/local/oracle/config/BIInstance/config/OracleBISchedulerComponent/coreapplication_obisch1
```

**On *FINHOST2*:**

```
/u02/local/oracle/config/BIInstance1/config/OracleBISchedulerComponent/
coreapplication_obisch1
```

You must update these files for each Oracle BI Scheduler component in the deployment.

- Restart the Oracle BI Scheduler component.

**On *FINHOST1*:**

```
$ cd /u02/local/oracle/config/BIInstance/bin
$./opmnctl stopproc
ias-component=coreapplication_obisch1
$./opmnctl startproc
ias-component=coreapplication_obisch1
```

**On *FINHOST2*:**

```
$ cd /u02/local/oracle/config/BIInstance1/bin
$./opmnctl stopproc
ias-component=coreapplication_obisch1
$./opmnctl startproc
ias-component=coreapplication_obisch1
```

### 15.5.6.2 Additional Configuration Tasks for Oracle Real-Time Decisions

This sections contains the following topics:

- [Section 15.5.6.2.1, "Configuring Oracle Real-Time Decisions Clustering Properties"](#)
- [Section 15.5.6.2.2, "Adding Oracle RTD System Properties to the Server Start Tab"](#)

**15.5.6.2.1 Configuring Oracle Real-Time Decisions Clustering Properties** Perform these steps in Fusion Middleware Control to set up cluster-specific configuration properties for Oracle RTD. You only need to perform the steps on one of the nodes in your deployment. You do not need to set cluster-specific configuration properties for Oracle RTD for subsequent nodes.

- Log in to Fusion Middleware Control (<http://biinternal.mycompany.com:7777/em>).
- Expand the **Application Deployments** node in the Farm\_BIDomain window.
- Expand **OracleRTD(11.1.1)(bi\_cluster)**.
- Click any node under it. For example, **OracleRTD(11.1.1)(bi\_server1)**.
- In the right pane, click **Application Deployment**, and then select **System MBean Browser**.
- In the System MBean Browser pane, expand **Application Defined MBeans**.
- For any one of the servers under OracleRTD, navigate to the MBean and set the attribute, as shown in [Table 15–1](#). Other servers automatically get updated with the value you set.

**Table 15–1 Oracle RTD MBean Attributes and Values for Clustering**

| MBean                            | Attribute              | Value                                                                                   |
|----------------------------------|------------------------|-----------------------------------------------------------------------------------------|
| SDClusterPropertyManager -> Misc | DecisionServiceAddress | <a href="http://biinternal.mycompany.com:7777">http://biinternal.mycompany.com:7777</a> |

- Click **Apply**.

**15.5.6.2.2 Adding Oracle RTD System Properties to the Server Start Tab** After scaling out Oracle RTD, use the Administration Console to add three system properties to the **Server Start** tab of each Managed Server.

1. Log in to the Oracle WebLogic Server Administration Console (<http://biinternal.mycompany.com:7777/console>).
2. Click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**.  
The Summary of Servers page displays.
5. Select **bi\_server<1,2>** in the table.  
The settings page for the server displays.
6. Click **Server Start**.
7. Add the following property to the arguments:
 

```
-Drttd.clusterRegistryJobIntervalMs=12000
-Drttd.clusterDepartureThresholdMs=50000
-Drttd.clusterDepartureThreshold2Ms=50000
```
8. Click **Save** and then **Activate Changes**.
9. Restart the **bi\_server<1,2>** Managed Server (ensure sure that Node Manager is up and running):
  - a. In the Summary of Servers screen, select the **Control** tab.
  - b. Select **bi\_server<1,2>** in the table and then click **Shutdown**.
  - c. Restart **bi\_server<1,2>**.
10. Restart the BI System Components:
 

```
$ cd /u02/local/oracle/config/BIInstance1/bin
$./opmnctl stopall
$./opmnctl startall
```

Performing this task enables an instance of Oracle RTD to be migrated successfully from one host to another in the event of a failure of a Managed Server.

Even after these changes, if the server migration finishes in less than 50 seconds, the Oracle RTD batch framework will be in an inconsistent state.

If the enterprise has deployed any RTD Inline Services that host Batch Job implementations, and if after a server migration the batch console command, "batch-names", or its brief name, "bn", shows no registered batch jobs, then the Oracle RTD Batch Manager service must be stopped and restarted. To do this, perform these steps:

1. In Fusion Middleware Control, expand the **WebLogic Domain** node in the left pane. Then, right-click **bifoundation\_domain** and select **System MBean Browser**.
2. Locate **SDPropertyManager > Misc MBean** under **Application Defined MBeans > OracleRTD > Server:bi\_servern**.  
Be sure to select the **Misc MBean** that corresponds to the local node where you are making the change. For example, if you are connecting to **APPHOST1**, then make sure to update the attribute associated with **bi\_server1**.
3. Set the **BatchManagerEnabled** attribute to **false** and click **Apply**.

4. Set the **BatchManagerEnabled** attribute back to **true** and click **Apply**. Performing this task causes the Batch Manager to stop and be restarted.

When it restarts, it will be running on either the same server as before, or on a different server.

5. After restarting Batch Manager, note that the corresponding MBean does not always immediately get refreshed on the server where Batch Manager comes back up, so this is not a concern. Instead, verify that Batch Manager is now operational by using the Batch Console tool:

- a. Locate the zip file for the Oracle RTD client tools in the following location:

`ORACLE_BASE/products/fusionapps/bi/clients/rtd/rtd_client_11.1.1.zip`

- b. Because most Oracle RTD client tools do not run on UNIX, unzip this file in a location on a Windows machine (referred to here as *RTD\_HOME*). Then, locate the batch console jar file in:

`RTD_HOME/client/Batch/batch-console.jar`

- c. Change to this directory and execute the jar, passing to it the URL and port of either the Managed Server, or of the cluster proxy:

```
java -jar batch-console.jar -url http://SERVER:PORT
```

- d. When prompted, enter the user name and password of a user who is a member of the Administrator role, BI\_Administrator role, or some other role authorized to administer Oracle RTD batch jobs.

- e. When prompted for a command, enter `bn`:

```
Checking server connection...
command: bn
 CrossSellSelectOffers
command:quit
```

If Batch Manager has successfully restarted, then the `bn` command lists the names of all batch implementations hosted by all deployed RTD Inline Services.

The commonly deployed example, `CrossSell`, hosts a batch implementation named `CrossSellSelectOffers`, shown in the preceding example.

### 15.5.6.3 Additional Configuration Tasks for Oracle BI Publisher

Perform the steps in this section on each machine where Oracle BI Publisher is configured.

This section includes the following topics:

- [Section 15.5.6.3.1, "Configuring Integration with Oracle BI Presentation Services"](#)
- [Section 15.5.6.3.2, "Setting the Oracle BI EE Data Source"](#)
- [Section 15.5.6.3.3, "Configuring JMS for BI Publisher"](#)

**15.5.6.3.1 Configuring Integration with Oracle BI Presentation Services** To configure Oracle BI Publisher integration with Oracle BI Presentation Services:

1. Log in to Oracle BI Publisher (<http://biinternal.mycompany.com:7777/xmlpserver>) with Administrator credentials and select the **Administration** tab.

2. Under **Integration**, select **Oracle BI Presentation Services**.
3. Verify and update the following:
  - **Server Protocol:** http
  - **Server:** biinternal.mycompany.com
  - **Port:** 7777
  - **URL Suffix:** analytics-ws/saw.dll
4. Click **Apply**.
5. Restart your Oracle BI Publisher application:
  - a. Log in to the Administration Console  
(http://biinternal.mycompany.com:7777/console).
  - b. Click **Deployments** in the Domain Structure window.
  - c. Select **bipublisher(11.1.1)**.
  - d. Click **Stop**, and then select **When Work Completes** or **Force Stop Now**.
  - e. After the application has stopped, click **Start** and then **Start Servicing All requests**.

**15.5.6.3.2 Setting the Oracle BI EE Data Source** The Oracle BI EE Data Source must point to the clustered Oracle BI Servers through the Cluster Controllers. Perform this task in Oracle BI Publisher.

To set the Oracle BI EE data source in Oracle BI Publisher:

1. Log in to Oracle BI Publisher  
(http://biinternal.mycompany.com:7777/xmlpserver) with Administrator credentials and select the **Administration** tab.
2. Under **Data Sources**, select **JDBC Connection**.
3. Update the Oracle BI EE data source setting by changing the **Connection String** parameter to the following:

```
jdbc:oraclebi://primary_cluster_controller_host:primary_cluster_controller_
port/PrimaryCCS=primary_cluster_controller_host;PrimaryCCSPort=primary_cluster_
controller_port;SecondaryCCS=secondary_cluster_controller_host;
SecondaryCCSPort=secondary_cluster_controller_port;
```

For example:

```
jdbc:oraclebi://FINHOST1:10212/PrimaryCCS=FINHOST1;PrimaryCCSPort=10212;
SecondaryCCS=FINHOST2;SecondaryCCSPort=10212;
```

---

**Note:** Since the Cluster Controller Port may be different between *FINHOST1* and *FINHOST2*, you can use the following procedure to check the port being used:

1. Log in to the Oracle Enterprise Manager Console:  
http://biinternal.mycompany.com:7777/em .
  2. Expand **Farm\_Domain** > **Business Intelligence** > **coreapplication**.
  3. Navigate to **Availability**.
  4. Check the port number used by the Cluster Controller on *FINHOST1* and *FINHOST2*.
-

4. Do one of the following:
  - Select **Use System User**.
  - Deselect **Use System User** and specify `BIImpersonateUser` credentials.

For more information, see "Credentials for Connecting to the Oracle BI Presentation Catalog" in *Oracle Fusion Middleware Developer's Guide for Oracle Business Intelligence Enterprise Edition*.
5. Click **Test Connection**. You should receive a "Connection established successfully" message.
6. Click **Apply**.

**15.5.6.3.3 Configuring JMS for BI Publisher** You must configure the location for all persistence stores to a directory visible from both nodes. Change all persistent stores to use this shared base directory.

On *FINHOST2*:

1. Log in to the Oracle WebLogic Server Administration Console (<http://biinternal.mycompany.com:7777/console>).
2. In the Domain Structure window, expand the **Services** node and then click the **Persistence Stores** node. The Summary of Persistence Stores page is displayed.
3. Click **Lock & Edit**.
4. Click **New**, and then **Create File Store**.
5. Enter a name (for example, `BipJmsStore2`) and target (for example, `bi_server2`). Enter a directory that is located in shared storage so that it is accessible from both *FINHOST1* and *FINHOST2*:  
  
`ORACLE_BASE/config/domains/ FINHOST1 /BIDomain/BipJmsStore`
6. Click **OK** and then **Activate Changes**.
7. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Servers** node. The Summary of JMS Servers page is displayed.
8. Click **Lock & Edit**.
9. Click **New**.
10. Enter a name (for example, `BipJmsServer2`) and in the **Persistence Store** drop-down list, select **BipJmsStore2** and click **Next**.
11. Select `bi_server2` as the target.
12. Click **Finish** and **Activate Changes**.
13. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Modules** node. The JMS Modules page is displayed.
14. In the Change Center, click **Lock & Edit**.
15. Click **BIPJmsResource** and then click the **Subdeployments** tab.
16. Select **BipJmsSubDeployment** under **Subdeployments**.
17. Add the new Oracle BI Publisher JMS Server (**BipJmsServer2**) as an additional target for the subdeployment.
18. Click **Save** and then **Activate Changes**.

To validate, do the following:

1. Log in to each Oracle BI Publisher URL.
2. Navigate to **System Maintenance > Administration > Scheduler Diagnostics**.  
All statuses should be in a Passed state and both instances should be visible.

#### 15.5.6.4 Additional Configuration Tasks for Oracle BI for Microsoft Office

This section includes the following topics:

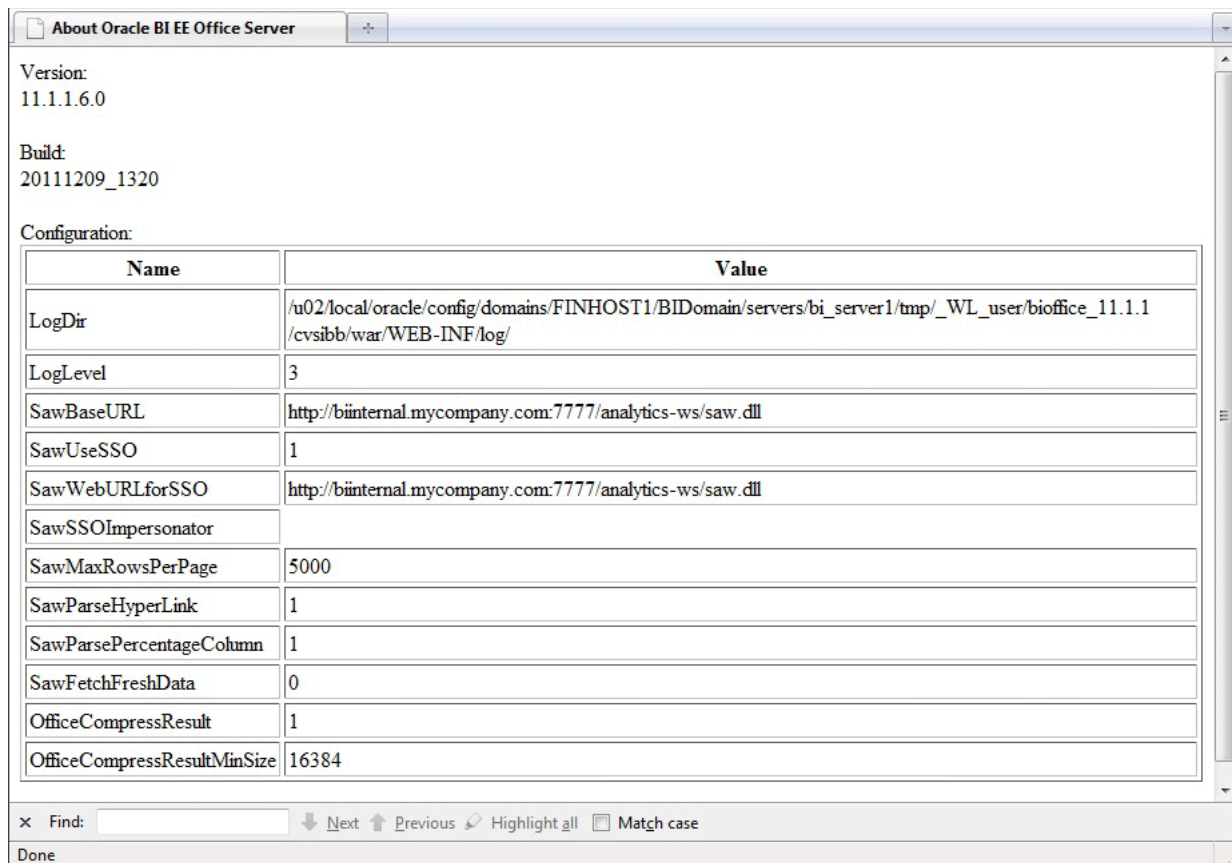
- [Section 15.5.6.4.1, "Configuring Oracle BI for Microsoft Office Properties"](#)
- [Section 15.5.6.4.2, "Validating Oracle BI for Microsoft Office"](#)

**15.5.6.4.1 Configuring Oracle BI for Microsoft Office Properties** To perform additional configuration tasks for Oracle BI for Microsoft Office:

1. Validate the Oracle BI Enterprise Edition Office Server setup by accessing `http://biinternal.mycompany.com:7777/bioffice/about.jsp`.

The About Oracle BI EE Office Server page is displayed, as shown in [Figure 15-1](#).

**Figure 15-1 About Oracle BI EE Office Server Page**



2. Go to the Oracle BI Enterprise Edition Office Server directory. For example:

`/u02/local/config/domains/FINHOST1/BIDomain/servers/bi_server1/tmp/_WL_user/bioffice_11.1.1/cvsibb/war/WEB-INF`

If you are not sure how to locate the Oracle BI Enterprise Edition Office Server directory, check the **LogDir** parameter on the About Oracle BI EE Office Server

page. The Oracle BI Enterprise Edition Office Server directory is the parent directory of the log directory.

---

**Note:** You can determine the exact location for *FINHOST<sub>n</sub>* by using the following URL: `http://BIVHn:10217/bioffice/about.jsp`.

---

3. On both *FINHOST1* and *FINHOST2*, open `bioffice.xml` for editing and modify the BI Office properties shown in [Table 15–2](#).

**Table 15–2 BI Office Properties in `bioffice.xml`**

| Property Name   | Valid Value                                                                                                                                         | Description                                                                                                                                                                                                                                                                                                                                                                                                          |
|-----------------|-----------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SawBaseURL      | <code>http://biinternal.mycompany.com:7777/analytics/saw.dll</code><br>or<br><code>http://biinternal.mycompany.com:7777/analytics-ws/saw.dll</code> | Load Balancer Virtual Server Name URL for Oracle BI Presentation Services.<br><br><b>Important:</b> If SSO is enabled, then enter the URL for the protected analytics servlet that you deployed when configuring BI Office to integrate with the SSO-enabled Oracle BI Server. The URL that is specified for this property is used for Web services requests between the BI Office Server and Presentation Services. |
| SawUseSSO       | 0 = No (Default)<br>1 = Yes                                                                                                                         | Set this property to 1 if the Oracle Business Intelligence implementation is enabled for SSO.                                                                                                                                                                                                                                                                                                                        |
| SawWebURLforSSO | <code>http://biinternal.mycompany.com:7777/analytics/saw.dll</code>                                                                                 | When SSO is enabled, use this property to enter the public URL that allows external users to access Oracle Business Intelligence using SSO from the Oracle BI Add-in for Microsoft Office.                                                                                                                                                                                                                           |

4. Restart the BI Office application:
  - a. Log in to the Administration Console (`http://biinternal.mycompany.com:7777/console`).
  - b. Click **Deployments** in the Domain Structure window.
  - c. Select **bioffice(11.1.1)**.
  - d. Click **Stop**.
  - e. After the application has stopped, click **Start**.
5. Validate that the **SawBaseURL** parameter has been updated on the About Oracle BI EE Office Server page.

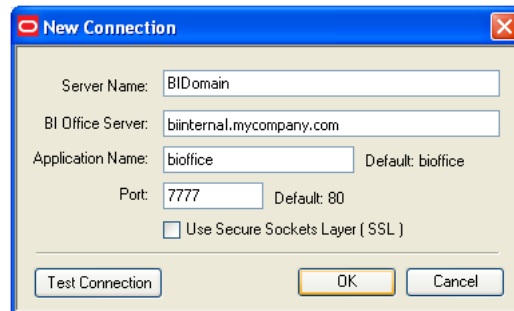
**15.5.6.4.2 Validating Oracle BI for Microsoft Office** To validate configuration for Oracle BI for Microsoft Office:

1. Log in to Oracle BI Presentation Services at:  
`http://biinternal.mycompany.com:7777/analytics`
2. In the lower left pane, under the Get Started heading, select **Download BI Desktop Tools** and then select **Oracle BI for MS Office**.

3. Install Oracle BI for Microsoft by running the Oracle BI Office InstallShield Wizard.
4. Open Microsoft Excel or Microsoft PowerPoint.
5. From the **Oracle BI** menu, select **Preferences**.
6. In the **Connections** tab, select **New**.
7. Enter values for the following fields:
  - **Server Name:** Provide a name for the connection.
  - **BI Office Server:** Provide the URL for the Oracle BI Office Server.
  - **Application Name:** Enter the Application Name that you defined for the Oracle BI Office Server when you deployed the Oracle BI Office Server application to WLS. The default name is **biooffice**.
  - **Port:** Enter the Oracle BI Office Server port number.

Figure 15–2 shows the New Connection dialog.

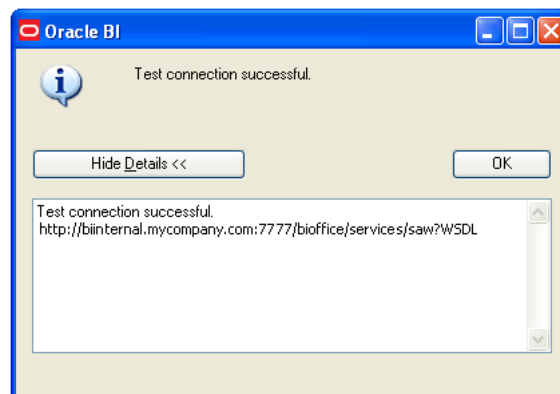
**Figure 15–2 New Connection Dialog for Oracle BI Office**



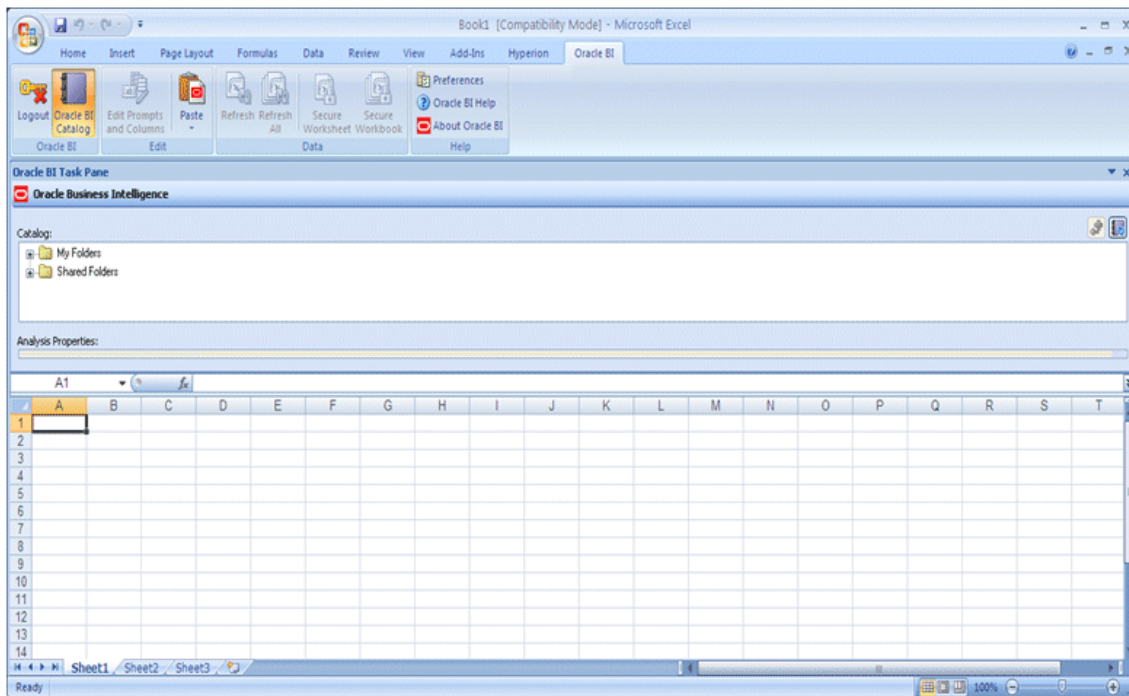
8. Click **Test Connection** to test the connection between the add-in and the Oracle BI Office Server.

Successful connections receive a "Test connection successful" message, as shown in Figure 15–3.

**Figure 15–3 Test Connection Successful Message**



9. Log in as an Administrator (for example, `weblogic`) and validate that you can access the Oracle BI Task Pane, as shown in Figure 15–4.

**Figure 15–4 Oracle BI Task Pane in Microsoft Excel**

#### 15.5.6.5 Additional Configuration Tasks for Oracle Financial Reporting

There are additional configuration tasks to perform for Oracle Financial Reporting. Do the following on *FINHOST1* and *FINHOST2*:

1. Update the `VARIABLE_VALUE_LIMIT` from 30720 to 3072000 in the `NQConfig.INI` file. For example,

```
VARIABLE_VALUE_LIMIT = 3072000;
```

On *FINHOST1*, this file is located in

```
/u02/local/oracle/config/BIIInstance/config/OracleBIServerComponent/core
application_obis1.
```

On *FINHOST2*, this file is located in

```
/u02/local/oracle/config/BIIInstance1/config/OracleBIServerComponent/cor
eapplication_obis1.
```

2. Run the following commands to restart the Oracle Business Intelligence system components:

```
$ cd /u02/local/oracle/config/BIIInstance/bin
$./opmnctl stopall
$./opmnctl startall
```

### 15.5.7 Configuring a Default Persistence Store for Transaction Recovery

Each server has a transaction log that stores information about committed transactions that are coordinated by the server that may not have been completed. The WebLogic Server uses this transaction log for recovery from system crashes or network failures. To leverage the migration capability of the Transaction Recovery Service for the servers within a cluster, store the transaction log in a location accessible to a server and its backup servers.

---

**Note:** Preferably, this location should be a dual-ported SCSI disk or on a Storage Area Network (SAN).

---

To set the location for the default persistence store:

1. Log in to the Oracle WebLogic Server Administration Console (<http://biinternal.mycompany.com:7777/console>).
2. In the Change Center, click **Lock & Edit**.
3. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node. The Summary of Servers page is displayed.
4. Click **bi\_server1** in the table. The Settings page for the selected server is displayed, and defaults to the Configuration tab.
5. Navigate to **Configuration > Services**.
6. In the Default Store section of the page, enter the path to the folder where the default persistent stores will store its data files. For example:

```
FINHOST1> ORACLE_BASE/config/domains/FINHOST1/BIDomain/tlogs
```

7. Click **Save**.
8. Repeat Steps 1 through 7 for the **bi\_server2** Managed Server.
9. Click **Activate Changes**.
10. Start the Managed Servers to activate the changes (ensure that Node Manager is up and running):
  - a. Log in to the Oracle WebLogic Server Administration Console (<http://biinternal.mycompany.com:7777/console>).
  - b. In the Summary of Servers screen, select the **Control** tab.
  - c. Select **bi\_server1** and **bi\_server2** in the table and then click **Shutdown**.
  - d. Start the **bi\_server1** and **bi\_server2** servers.
  - e. Restart the Oracle Business Intelligence system components:

```
$ cd /u02/local/oracle/config/BIInstancen/bin
$./opmnctl stopall
$./opmnctl startall
```

---

**Note:** To enable migration of the Transaction Recovery service, specify a location on a persistent storage solution that is available to other servers in the cluster. Both **bi\_server1** and **bi\_server2** must be able to access this directory.

---

## 15.5.8 Starting and Validating Oracle Business Intelligence on FINHOST2

This section includes the following topics:

- [Section 15.5.8.1, "Starting the bi\\_server2 Managed Server"](#)
- [Section 15.5.8.2, "Starting the Oracle Business Intelligence System Components"](#)
- [Section 15.5.8.3, "Validating Oracle Business Intelligence URLs"](#)

### 15.5.8.1 Starting the bi\_server2 Managed Server

To start the bi\_server2 Managed Server:

1. Start the bi\_server2 Managed Server using the Oracle WebLogic Server Administration Console, as follows:
  - a. Log in to the Oracle WebLogic Server Administration Console (<http://biinternal.mycompany.com:7777/console>).
  - b. Expand the **Environment** node in the **Domain Structure** window.
  - c. Select **Servers**. The Summary of Servers page is displayed.
  - d. Click the **Control** tab.
  - e. Select **bi\_server2** 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.

### 15.5.8.2 Starting the Oracle Business Intelligence System Components

You can control Oracle Business Intelligence system components using opmnctl commands.

To start the Oracle Business Intelligence system components using the opmnctl command-line tool:

1. Go to the directory that contains the Oracle Process Manager and Notification Server command-line tool, located in  
`/u02/local/oracle/config/BIInstance1/bin.`
2. Run the opmnctl command to start the Oracle Business Intelligence system components:
  - `./opmnctl startall`: Starts Oracle Process Manager and Notification Server and all Oracle Business Intelligence system components
  - `./opmnctl start`: Starts Oracle Process Manager and Notification Server only
  - `./opmnctl startproc ias-component=component_name`: Starts a particular system component. For example, where `coreapplication_obips1` is the Presentation Services component:  
  
`./opmnctl startproc ias-component=coreapplication_obips1`
3. Check the status of the Oracle Business Intelligence system components:  
  
`./opmnctl status`

### 15.5.8.3 Validating Oracle Business Intelligence URLs

Access the following URLs:

- Access <http://BIVH2:10217/analytics> to verify the status of bi\_server2.
- Access <http://BIVH2:10217/wsm-pm> to verify the status of Web Services Manager. Click **Validate Policy Manager**. A list of policies and assertion templates available in the data is displayed.

**Note:** The configuration is incorrect if no policies or assertion templates appear.

- Access <http://BIVH2:10217/xmlpserver> to verify the status of the Oracle BI Publisher application.

- Access <http://BIVH2:10217/ui> to verify the status of the Oracle Real-Time Decisions application.
- Access <http://BIVH2:10217/mapviewer> to verify the status of the map view functionality in Oracle BI EE.
- Access <http://BIVH2:10217/hr> to verify Financial Reporting.
- Access <http://BIVH2:10217/calcmgr/index.htm> to verify Calculation Manager.
- Access <http://BIVH2:10217/aps/Test> to verify APS.
- Access <http://BIVH2:10217/workspace> to verify workspace.

### 15.5.9 Validating Access Through Oracle HTTP Server

You should verify URLs to ensure that the appropriate routing and failover is working from Oracle HTTP Server to `bi_cluster`. Perform these steps to verify the URLs:

1. While `bi_server2` is running, stop `bi_server1` using the Oracle WebLogic Server Administration Console.
2. Access the following URLs to verify that routing and failover is functioning properly:
  - <http://WEBHOST1:10621/analytics>
  - <http://WEBHOST1:10621/xmlpserver>
  - <http://WEBHOST1:10621/ui> (access only available on Microsoft Internet Explorer 7 or 8)
  - <http://WEBHOST1:10621/hr>
  - <http://WEBHOST1:10621/calcmgr/index.htm>
  - <http://WEBHOST1:10621/aps/Test>
  - <http://WEBHOST1:10621/workspace>
3. Start `bi_server1` from the Oracle WebLogic Server Administration Console.
4. Stop `bi_server2` from the Oracle WebLogic Server Administration Console.
5. Access the following URLs to verify that routing and failover is functioning properly:
  - <http://WEBHOST1:10621/analytics>
  - <http://WEBHOST1:10621/xmlpserver>
  - <http://WEBHOST1:10621/ui> (access only available on Microsoft Internet Explorer 7 or 8)
  - <http://WEBHOST1:10621/hr>
  - <http://WEBHOST1:10621/calcmgr/index.htm>
  - <http://WEBHOST1:10621/aps/Test>
  - <http://WEBHOST1:10621/workspace>
6. Start `bi_server2` from the Oracle WebLogic Server Administration Console.

### 15.5.10 Configuring Node Manager for the Managed Servers

Oracle recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for

the different addresses communicating with the Administration Server and other servers. See [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"](#) for further details. The procedures in that chapter must be performed twice using the information provided in [Table 15–3](#).

**Table 15–3 Details for Host Name Verification for Node Manager and Servers**

| Run   | Host Name (Host) | Server Name (WLS_SERVER) |
|-------|------------------|--------------------------|
| Run1: | <i>FINHOST1</i>  | bi_server1               |
| Run2: | <i>FINHOST2</i>  | bi_server2               |

---

**Note:** If you configured Node Manager for the Managed Servers earlier, you do not need to configure it again.

---

### 15.5.11 Configuring Server Migration for the Managed Servers

Server Migration is required for proper failover of the Oracle BI Publisher components in the event of failure in any of the *FINHOST1* and *FINHOST2* nodes. For more information, see [Chapter 18, "Setting Up Server Migration for an Enterprise Deployment."](#)

## 15.6 Configuring Oracle Essbase Clustering

This section describes how to configure secondary instances of Oracle Essbase Agent so that they are distributed for high availability.

### Prerequisite steps for configuring Oracle Essbase clustering:

1. On *FINHOST1* or *FINHOST2*, delete or rename the `EssFOConfig.properties` file in the Essbase shared folder under `ORACLE_BASE/config/BIShared/Essbase/essbaseserver1`.
2. On *FINHOST1*, update the following properties in the `/u02/local/oracle/config/BIInstance/bin/essbase_ha/EssFOConfig.properties` file:

```
SYSTEM_HOST=FINHOST1
SYSTEM_HOST1=FINHOST1
SYSTEM_HOST2=FINHOST2

SYSTEM_CLUSTER_NAME=essbasecluster1
SYSTEM_CLUSTER_INST1=essbasecluster1-inst1
SYSTEM_CLUSTER_INST2=essbasecluster1-inst2

SYSTEM_CLUSTER_INSTANCE1=BIInstance
SYSTEM_CLUSTER_INSTANCE2=BIInstance1

SYSTEM_AGENT_PORTNUMBER1=10215
SYSTEM_AGENT_PORTNUMBER2=10215
```

Perform the following steps in Fusion Middleware Control:

1. Log in to Fusion Middleware Control (<http://biinternal.mycompany.com:7777/em>).
2. Expand the **Business Intelligence** node in the `Farm_BIDomain` window.

3. Click **coreapplication**.
4. Click **Availability**, then click **Failover**.
5. Click **Lock and Edit Configuration** to activate the Primary/Secondary Configuration section of the **Availability** tab.
6. Specify the Secondary Host/Instance for Essbase Agent.
7. Ensure the **Shared Folder Path** is set to `ORACLE_BASE/config/BIShared/Essbase/essbaseserver1` and click **Apply**.  
Under Potential Single Points of Failure, no problems should be reported for Essbase Agent.
8. Click **Activate Changes**.
9. Under Manage System, click **Restart**.
10. Click **Yes** in the confirmation dialog.

### 15.6.1 Validating Essbase Clustering

Do the following to validate Essbase clustering:

1. Check the APS (Hyperion Provider Services) test URL:  
`http://biinternal.mycompany.com:7777/aps/Test`
2. Run the following command on *FINHOST1*:  

```
/u02/local/oracle/config/BIInstance/bin/opmnctl stopproc
ias-component=essbasecluster1
```
3. Ensure that Essbase starts on *FINHOST2*:  

```
/u02/local/oracle/config/BIInstance1/bin/opmnctl status
```

  
The status should be `init` then `Alive`.
4. Check the APS test URL again:  
`http://biinternal.mycompany.com:7777/aps/Test`

## 15.7 Validating the System

You should verify URLs to ensure that the appropriate routing and failover is working from Oracle HTTP Server to `bi_cluster`. Perform these steps to verify the URLs:

1. While `bi_server2` is running, stop `bi_server1` using the Oracle WebLogic Server Administration Console.
2. Access the following URLs to verify that routing and failover is functioning properly:
  - `http://WEBHOST1:10621/analytics`
  - `http://WEBHOST1:10621/xmlpserver`
  - `http://WEBHOST1:10621/ui` (access only available on Microsoft Internet Explorer 7 or 8)
  - `http://WEBHOST1:10621/hr`
  - `http://WEBHOST1:10621/workspace`
  - `http://WEBHOST1:10621/calcmgr/index.htm`

- <http://WEBHOST1:10621/aps/Test>
- 3. Start `bi_server1` from the Oracle WebLogic Server Administration Console.
- 4. Stop `bi_server2` from the Oracle WebLogic Server Administration Console.
- 5. Access the following URLs to verify that routing and failover is functioning properly:
  - <http://WEBHOST1:10621/analytics>
  - <http://WEBHOST1:10621/xmlpserver> (access only available on Microsoft Internet Explorer 7 or 8)
  - <http://WEBHOST1:10621/ui>
  - <http://WEBHOST1:10621/hr>
  - <http://WEBHOST1:10621/workspace>
  - <http://WEBHOST1:10621/calcmgr/index.htm>
  - <http://WEBHOST1:10621/aps/Test>
- 6. Start `bi_server1` from the Oracle WebLogic Server Administration Console.

---

## Additional Configuration Procedures for Scaling Out Oracle SOA Suite Server

---

This chapter describes the additional scaleout steps required for the `soa_server1` and `soa_server2` server on `FINHOST1` and `FINHOST2`.

---

**Note:** The Oracle SOA Suite server uses the Java Message Service (JMS) server. JMS requires a shared file system for its file store and transactional log. Each Oracle SOA Suite Managed Server in a cluster uses a separate local file system on the shared disk. During a node failure, the Oracle SOA Suite server must be moved to a targeted node in order to run the same server using the exact JMS file store and transaction log. To enable this server migration, each Oracle SOA Suite server must be configured with its own virtual IP, which can be floated on any server where the Oracle SOA Suite server is migrated.

---

The procedures in this chapter use the Oracle SOA Suite server in the Oracle Fusion Financials domain as an example. You must perform the same procedures for the Oracle SOA Suite servers in all other domains.

---

**Note:** For Oracle Fusion Financials, the Oracle SOA Suite virtual IPs for `FINHOST1` and `FINHOST2` are called `FINSOAVH1` and `FINSOAVH2`. For all other domains, replace the first three characters with domain-specific syntax. For `HCMOAVH1`, `SCMSOAVH1`, and so on.

---

This chapter includes the following topics:

- [Section 16.1, "Enabling Virtual IPs on FINHOST1 and FINHOST2"](#)
- [Section 16.2, "Setting the Listen Address for soa\\_server1"](#)
- [Section 16.3, "Setting the Listen Address for soa\\_server2"](#)
- [Section 16.4, "Updating the FusionVirtualHost\\_fin.conf Configuration File"](#)
- [Section 16.5, "Configuring JMS for the Oracle SOA Suite Server"](#)
- [Section 16.6, "Configuring Oracle Coherence for Deploying Composites"](#)
- [Section 16.7, "Configuring a Default Persistence Store for Transaction Recovery"](#)
- [Section 16.8, "Disabling Host Name Verification for the soa\\_servern Managed Servers"](#)
- [Section 16.9, "Restarting Node Manager on FINHOST1"](#)

- [Section 16.10, "Starting and Validating soa\\_server1 on FINHOST1"](#)
- [Section 16.11, "Restarting Node Manager on FINHOST2"](#)
- [Section 16.12, "Starting and Validating soa\\_server2 on FINHOST2"](#)

---

**Note:** Before performing any of the procedures in this chapter, ensure that `soa_server1` is running on *FINHOST1* and `soa_server2` is running on *FINHOST2*.

---

## 16.1 Enabling Virtual IPs on FINHOST1 and FINHOST2

To enable the virtual IP on Linux:

---

**Note:** In this example, `ethX` is the ethernet interface (`eth0` or `eth1`) and `Y` is the index (0, 1, 2, and so on). In addition, the *FINSOAVH1* and *FINSOAVH2* VIPs will be used.

---

1. On *FINHOST1*:
  - a. Run the `ifconfig` command as root:

```
/sbin/ifconfig interface:index IPAddress netmask netmask
```

For example:

```
/sbin/ifconfig ethX:Y 100.200.140.206 netmask 255.255.255.0
```
  - b. Enable your network to register the new location of the virtual IP:

```
/sbin/arping -q -U -c 3 -I interface IPAddress
```

For example:

```
/sbin/arping -q -U -c 3 -I ethX 100.200.140.206
```
  - c. Validate that the address is available by pinging it from another node.

For example:

```
/bin/ping 100.200.140.206
```
2. Repeat Steps a through c on *FINHOST2*.

## 16.2 Setting the Listen Address for soa\_server1

Ensure that you have performed the steps described in [Section 16.1](#), and the scale-out steps described in [Section 8.3](#), [Section 8.4](#), and [Section 8.5](#) before setting the `soa_server1` listen address.

To set the listen address for the Managed Server:

1. Log in to the Administration Console.
2. In the Change Center, click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select `soa_server1` in the table. The Setting page for `soa_server1` is displayed.

6. Set the **Listen Address** to *FINSOAVH1*.
7. Click **Save**.
8. Click **Activate Changes**.
9. The changes will not take effect until the *soa\_server1* Managed Server is restarted (ensure that Node Manager is up and running):
  - a. On the Summary of Servers page, select the **Control** tab.
  - b. Select *soa\_server1* in the table and then click **Shutdown**.
  - c. After the server has shut down, select *soa\_server1* in the table and then click **Start**.

## 16.3 Setting the Listen Address for *soa\_server2*

Ensure that you have performed the steps described in [Section 16.1](#) before setting the *soa\_server2* listen address.

Perform these steps to set the listen address for the Managed Server:

1. Log in to the Administration Console.
2. In the Change Center, click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select *soa\_server2* in the column of the table. The Settings page for *soa\_server2* is displayed.
6. Set the **Listen Address** to *FINSOAVH2*.
7. Click **Save**.
8. Click **Activate Changes**.
9. The changes will not take effect until the *soa\_server2* Managed Server is restarted (ensure that Node Manager is up and running):
  - a. On the Summary of Servers page, select the **Control** tab.
  - b. Select *soa\_server2* in the table and then click **Shutdown**.
  - c. After the server has shut down, select *soa\_server2* in the table and then click **Start**.

## 16.4 Updating the FusionVirtualHost\_fin.conf Configuration File

To enable Oracle HTTP Server to route to *soa\_cluster*, which contains the *soa\_servern* Managed Servers, you must set the WebLogicCluster parameter to the list of nodes in the cluster.

To set the parameter:

1. On *WEBHOST1* and *WEBHOST2*, update the WebLogicCluster parameter in the *ORACLE\_BASE/config/CommonDomain\_webtier/config/OHS/ohs1/moduleconf/FusionVirtualHost\_fin.conf* file to contain a cluster list of virtual *host:port* entries. For example:

```
<Location /soa-infra>
 SetHandler weblogic-handler
 WebLogicCluster FINSOAVH1:7416,FINSOAVH2:7416
```

```
</Location>
```

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

```
WEBHOST1> ORACLE_BASE/config/CommonDomain_webtier/bin/opmnctl restartproc
ias-component=ohs1
```

```
WEBHOST2> ORACLE_BASE/config/CommonDomain_webtier/bin/opmnctl restartproc
ias-component=ohs1
```

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

Sample scenarios include the following:

- **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 dynamically 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 the members of the cluster, then you guarantee you can route to the cluster, assuming at least one member is running when Oracle HTTP Server is started. For more information on configuring the Oracle WebLogic Server plug-in, see *Oracle Fusion Middleware Using Web Server 1.1 Plug-Ins with Oracle WebLogic Server*.

## 16.5 Configuring JMS for the Oracle SOA Suite Server

After *FINHOST1* has been provisioned, the JMS server and file store are set up and configured for *FINHOST1*. You now must configure the file store for *FINHOST2*. Configure the location for all persistence stores to a directory visible from both nodes.

To configure the file store for *FINHOST2*:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand the **Services** node and then click the **Persistence Stores** node.

The Summary of Persistence Stores page appears.

3. Click **Lock & Edit**.
4. Click **New**, and then **Create File Store**.
5. In the Directory field, enter the following:
  - Name: for example, SOAJMSFileStore\_auto\_2
  - Target: soa\_server2
  - Directory:

```
ORACLE_BASE/config/domains/FINHOST1/FinancialDomain
```

6. Click **OK** and **Activate Changes**.

7. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Servers** node.

The Summary of JMS Servers page appears.

8. Click **Lock & Edit**.
9. Click **New**.
10. Enter a name (for example, `SOAJMSServer_2`), then select **SOAJMSFileStore\_auto\_2** in the Persistence Store dropdown list.
11. Click **Next**.
12. Select `soa_server2` as the target.
13. Click **Finish** and **Activate Changes**.
14. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Modules** node.

The JMS Modules page appears.
15. In the Change Center, click **Lock & Edit**.
16. Click **SOAJMSModule** and then click the **Subdeployments** tab.
17. Click **SOAJMSServerxxxxx** under **Subdeployments**.
18. Add the new `SOAJMSServer_2` as additional targets for the subdeployment.
19. Click **Save** and **Activate Changes**.

## 16.6 Configuring Oracle Coherence for Deploying Composites

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

---

---

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

---

---

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

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

Specify the nodes using the `tangosol.coherence.wka.n` system property, where *n* is the number for each Oracle HTTP Server. The numbering starts at 1. This numbering must be sequential and must not contain gaps. In addition, specify the host name used by Oracle Coherence to create a cluster through the `tangosol.coherence.localhost` system property. This local host name should be the virtual host name used by the SOA server as the listener addresses (*FINSOAVH1* and *FINSOAVH2*). Set this property by adding the `-Dtangosol.coherence.localhost` parameters to the Arguments field of the Oracle WebLogic Server Administration Console's Server Start tab.

---

**Note:** *FINSOAVH1* is the virtual host name that maps to the virtual IP where `soa_server1` is listening (in *FINHOST1*). *FINSOAVH2* is the virtual host name that maps to the virtual IP where `soa_server2` is listening (in *FINHOST2*).

---

To add the host name used by Oracle Coherence:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand the **Environment** node.
3. Click **Servers**.  
The Summary of Servers page appears.
4. Select **soa\_server1** (represented as a hyperlink) from the column of the table.  
The Settings page appears.
5. Click **Lock & Edit**.
6. Click the **Server Start** tab.
7. Enter the following for `soa_server1` and `soa_server2` into the **Arguments** field.

For `soa_server1`, enter the following:

```
-Dtangosol.coherence.wka1=FINSOAVH1
-Dtangosol.coherence.wka2=FINSOAVH2
-Dtangosol.coherence.localhost=FINSOAVH1
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
```

For `soa_server2`, enter the following:

```
-Dtangosol.coherence.wka1=FINSOAVH2
-Dtangosol.coherence.wka2=FINSOAVH1
-Dtangosol.coherence.localhost=FINSOAVH2
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
```

---

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

---

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

---

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

---



---

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

---



---

**Note:** The Oracle Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying the `-Dtangosol.coherence.wkaX.port` startup parameter.

---

## 16.7 Configuring a Default Persistence Store for Transaction Recovery

Each server has a transaction log that stores information about committed transactions that are coordinated by the server that may not have been completed. The WebLogic Server uses this transaction log for recovery from system crashes or network failures. To leverage the migration capability of the Transaction Recovery Service for the servers within a cluster, store the transaction log in a location accessible to a server and its backup servers.

---

**Note:** Preferably, this location should be a dual-ported SCSI disk or on a Storage Area Network (SAN).

---

To set the location for the default persistence store:

1. Log in to the Oracle WebLogic Server Administration Console (<http://fininternal.mycompany.com:7777/console>).
2. In the Change Center, click **Lock & Edit**.
3. In the Domain Structure window, expand the **Environment** node and then click the **Servers** node. The Summary of Servers page is displayed.
4. Click the server name **soa\_server1** (represented as a hyperlink) in the table. The Settings page for the selected server is displayed, and defaults to the Configuration tab.
5. Click the **Configuration** tab and then the **Services** tab.
6. In the Default Store section of the page, enter the path to the folder where the default persistent stores will store its data files. The directory structure of the path for *FINHOST1* is the following:

```
FINHOST1> ORACLE_BASE/config/domains/FINHOST1/FinancialDomain/tlogs
```

7. Repeat Steps 4 through 6 for **soa\_server2**.
8. Click **Save** and **Activate Changes**.
9. Restart the Managed Servers to activate the changes (ensure that Node Manager is up and running):
  - a. Log in to the Oracle WebLogic Server Administration Console (<http://fininternal.mycompany.com:7777/console>).
  - b. In the Summary of Servers screen, select the **Control** tab.
  - c. Select **soa\_server1** and **soa\_server2** in the table and then click **Shutdown**.
  - d. Start the **soa\_server1** and **soa\_server2** servers.

---

**Note:** To enable migration of the Transaction Recovery service, specify a location on a persistent storage solution that is available to other servers in the cluster. Both **soa\_server1** and **soa\_server2** must be able to access this directory.

---

## 16.8 Disabling Host Name Verification for the soa\_servern Managed Servers

This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server. By default, Host Name Verification should be set to *None*. If it is not, follow the steps below.

If you have not configured the server certificates, you will receive errors when managing the different WebLogic servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again once the enterprise deployment topology configuration is complete.

To disable Host Name Verification:

1. Log in to Oracle WebLogic Server Administration Console. For example, <http://fininternal.mycompany.com:7777/console>.
2. Click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**.

The Summary of Servers page appears.

5. Select **soa\_server1** (represented as a hyperlink) in the table.

The Settings page appears.

6. Select the **SSL** tab.
7. Expand the **Advanced** section of the page.
8. Set **Hostname Verification** to **None**.
9. Click **Save**.
10. Repeat Steps 1 through 9 for the **soa\_server2** Managed Server.
11. Save and activate the changes.

## 16.9 Restarting Node Manager on FINHOST1

To restart Node Manager on *FINHOST1*:

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

```
FINHOST1> ps -ef | grep NodeManager
orcl 9139 9120 0 Mar03 pts/6 00:00:00/bin/sh ./startNodeManager.sh
```

- c. Run the following command:

```
FINHOST1>kill -9 9139
```

2. Start Node Manager:

```
FINHOST1> ORACLE_BASE/products/fusionapps/wlserver_10.3/common/nodemanager/
FINHOST1/startNodeManagerWrapper.sh
```

## 16.10 Starting and Validating soa\_server1 on FINHOST1

To start the *soa\_server1* Managed Server on *FINHOST1*:

1. Access the Administration Console. For example, <http://fininternal.mycompany.com:7777/console>.
2. Click **Servers**.
3. Open the **Control** tab.
4. Select **soa\_server1**.
5. Click **Start**.

To validate the *soa\_server1* Managed Server on *FINHOST1*:

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. Access <http://FINSOAVH1:7416/soa-infra> and <http://fininternal.mycompany.com:7777/soa-infra> to verify status of *soa\_server1*.

---

**Note:** Although the *soa\_server1* server may be up, some applications may be in a failed state. Therefore, Oracle recommends verifying the above URLs and watching for errors pertaining each individual application in the server's output file.

---

## 16.11 Restarting Node Manager on FINHOST2

To restart Node Manager on *FINHOST2*, follow the steps in [Section 16.9, "Restarting Node Manager on FINHOST1."](#)

## 16.12 Starting and Validating soa\_server2 on FINHOST2

To start the soa\_server2 Managed Server on *FINHOST2* and ensure that it is configured correctly:

1. From the Administration Console, start the soa\_server2 Managed Server.
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.
3. Access <http://FINSOAVH2:7416/soa-infra> and <http://fininternal.mycompany.com:7777/soa-infra>.

---

**Note:** Although soa\_server2 server may be up, some applications may be in a failed state. Therefore, Oracle recommends verifying the above URLs and watching for errors pertaining each individual application in the server's output file.

---

---

# Configuring Administration Server High Availability

This chapter describes how to configure and validate the Oracle WebLogic Server Administration Server for high availability.

This chapter includes the following topics:

- [Section 17.1, "Enabling Administration Server High Availability"](#)
- [Section 17.2, "Oracle HTTP Server Configuration"](#)
- [Section 17.3, "Validating the Administration Server"](#)
- [Section 17.4, "Manually Failing Over the Administration Server to FINHOST2"](#)
- [Section 17.5, "Failing the Administration Server Back to FINHOST1"](#)

## 17.1 Enabling Administration Server High Availability

The Administration Server is a singleton application, so it cannot be deployed in an active-active configuration. By default, the Administration Server is only available on the first installed node. If this node becomes unavailable, then the Administration Console and Fusion Middleware Control also become unavailable. To avoid this scenario, the Administration Server and the applications deployed to it must be enabled for failover. The enterprise deployment architecture in this guide calls for the deploying the Administration Server on a disk shared between the primary node and the secondary node.

The following domains are deployed as part of the Oracle Fusion Financials enterprise deployment implementation:

- Oracle Fusion Customer Relationship Management Domain
- Oracle Fusion Common Domain
- Oracle Fusion Financials Domain
- Oracle Fusion Human Capital Management Domain
- Oracle Fusion Supply Chain Management Domain
- Oracle Fusion Projects Domain
- Oracle Fusion Procurement Domain
- Oracle Business Intelligence Domain

The process described in this guide initially deploys each domain-specific Administration Server in shared storage (/u01/oracle) mounted on *FINHOST1*, and Managed Servers in the local disk (/u02/local/oracle).

This section contains the following topics:

- [Section 17.1.1, "Enabling Administrative Virtual Host on FINHOST1"](#)
- [Section 17.1.2, "Adding a New Machine in the Oracle WebLogic Server Console"](#)
- [Section 17.1.3, "Enabling the Administration Server to Listen on the Virtual IP Address"](#)

## 17.1.1 Enabling Administrative Virtual Host on FINHOST1

---

**Note:** *FINADMINVH* is used as a generic name in this chapter. For domain-specific administrative virtual host names, see [Table 3-1](#) in [Section 3.6, "IPs and Virtual IPs."](#)

---

The Administration Server must be configured to listen on a virtual IP Address to enable it to seamlessly failover from one host to another. In case of a failure, the Administration Server, along with the virtual IP Address, can be migrated from one host to another.

However, before the Administration Server can be configured to listen on a virtual IP Address, one of the network interface cards on the host running the Administration Server must be configured to listen on this virtual IP Address. The steps to enable a virtual IP Address are completely dependent on the operating system.

To enable a virtual IP Address on *FINHOST1*:

---

**Note:** In a UNIX environment, the command must be run as the root user.

---

1. On *FINHOST1*, run the `ifconfig` command to get the value of the netmask. In a UNIX environment, run this command as the root user. For example:

```
[root@FINHOST1 ~] # /sbin/ifconfig
eth0 Link encap:Ethernet HWaddr 00:11:43:D7:5B:06
 inet addr:139.185.140.51 Bcast:139.185.140.255 Mask:255.255.255.0
 inet6 addr: fe80::211:43ff:fed7:5b06/64 Scope:Link
 UP BROADCAST RUNNING MULTICAST MTU:1500 Metric:1
 RX packets:10626133 errors:0 dropped:0 overruns:0 frame:0
 TX packets:10951629 errors:0 dropped:0 overruns:0 carrier:0
 collisions:0 txqueuelen:1000
 RX bytes:4036851474 (3.7 GiB) TX bytes:2770209798 (2.5 GiB)
 Base address:0xeccc Memory:dfae0000-dfb00000
```

2. On *FINHOST1*, bind the virtual IP Address to the network interface card using `ifconfig`. In a UNIX environment, run this command as the root user. Use a netmask value that was obtained in Step 1.

The syntax and usage for the `ifconfig` command is as follows:

```
/sbin/ifconfig networkCardInterface Virtual_IP_Address netmask netMask
```

For example:

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

3. Update the routing table using `arping`. In a UNIX environment, run this command as the root user.

```
/sbin/arping -q -U -c 3 -I networkCardInterface Virtual_IP_Address
```

For example:

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

## 17.1.2 Adding a New Machine in the Oracle WebLogic Server Console

Create a new machine and assign the Administration Server to the new machine using the Administration Console:

1. Log in to the Administration Console.
2. In the Change Center, click **Lock & Edit**.
3. In the Environment section of the Home page, click **Machines**.
4. On the Summary of Machines page, select the machine that is associated with the Administration Server from under the **Machines** table and click **Clone**. For example: `FINHOST1.MYCOMPANY.COM`.
5. On the Clone a Machine page, enter the name of the machine under the Machine Identity section and click **OK**. For example, enter `ADMINHOST` as the machine name.
6. On the Summary of Machines page, click the newly created machine link.
7. On the Settings page for the `ADMINHOST` machine, select the **Servers** tab.
8. Click **Add** under the **Servers** table.
9. On the Add a Server to Machine page, select **Select an existing server**, and associate it with this machine option.
10. Choose the AdminServer from the dropdown list.
11. Click **Finish** to associate the Administration Server with the machine.
12. In the Change Center, click **Activate Changes**.

## 17.1.3 Enabling the Administration Server to Listen on the Virtual IP Address

Ensure that you have performed the steps described in [Section 17.1.1, "Enabling Administrative Virtual Host on FINHOST1"](#) before setting the Administration Server listen address.

To set the Administration Server listen address:

1. Log in to the Administration Console.
2. In the Change Center, click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select **AdminServer(admin)** in the table. The Settings page for AdminServer(admin) is displayed.
6. Set the **Listen Address** to `FINADMINVH` (domain-specific administrative virtual host).
7. Click **Save**.

8. Click **Activate Changes**.
9. The changes will not take effect until the Administration Server is restarted. Follow these steps to restart the Administration Server:
  - a. In the Summary of Servers page, select the **Control** tab.
  - b. Select **AdminServer(admin)** in the table and then click **Shutdown**.
10. Set the following environment variable:

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks"
```
11. Start the Administration Server again from the command line. Use the nmconnect username and password you specified in the [Installation Location Screen](#) in [Chapter 5](#).

```
FINHOST1> ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin/wlst.sh
```

```
FINHOST1> nmConnect(username='username', password='password',
domainName='domain_name', host='FINHOST1',port='5556', nmType='ssl',
domainDir='ORACLE_BASE/config/domains/FINHOST1/domain_name')
```

```
FINHOST1> nmStart('AdminServer')
```

## 17.2 Oracle HTTP Server Configuration

To configure Oracle HTTP Server:

1. On *WEBHOST1*:
  - a. `cd ORACLE_BASE/config/CommonDomain_webtier/config/OHS/ohs1/moduleconf.`
  - b. Edit the domain-specific virtual host config file. For example:

```
cp FusionVirtualHost_fin.conf FusionVirtualHost_fin.conf.org
```
2. Edit the `FusionVirtualHost_fin.conf` file, adding the Administrative virtual host and port. [Example 17–1](#) shows sample code.

---

---

**Note:** Replace *FINADMINVH* and port with domain-specific Administrative virtual host and port number.

---

---

### **Example 17–1 Add AdministrativeVirtual Host and Port**

```
Context roots for application em
<Location /em>
 SetHandler weblogic-handler
 WebLogicCluster FINADMINVH:port
</Location>

Context roots for application console
<Location /console >
 SetHandler weblogic-handler
 WebLogicCluster FINADMINVH:port
</Location>
```

3. Restart Oracle HTTP Server: `cd to ORACLE_BASE/config/CommonDomain_webtier/bin` and enter the following:

```
WEBHOST1> ./opmnctl stopall
WEBHOST1> ./opmnctl startall
```

4. Repeat Steps 1 through 3 on *WEBHOST2*.

## 17.3 Validating the Administration Server

Perform these steps to ensure that the Administration Server and Oracle Enterprise Manager Fusion Middleware Control are properly configured:

1. Ensure that you can access the domain-specific Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control. For example, for the Oracle Fusion Financials domain:

```
http://fininternal.mycompany.com:7777/console
```

```
http://fininternal.mycompany.com:7777/em
```

2. After completing the steps in [Section 17.1](#) and [Section 17.2](#) for other domains, repeat Step 1 for other domains by replacing the domain-specific URL.

## 17.4 Manually Failing Over the Administration Server to FINHOST2

In case a node fails, you can fail over the Administration Server to another node. This section describes how to fail over the Administration Server from *FINHOST1* to *FINHOST2*.

### 17.4.1 Prerequisites

Ensure the following:

- The Administration Server is configured to listen on a domain-specific administrative virtual host, and not on **any** address
- When failover happens, the Administration Server is failed over from *FINHOST1* to *FINHOST2* and the two nodes have the following IPs:
  - *FINHOST1* to : 100.200.140.165
  - *FINHOST2*: 100.200.140.205
  - *FINADMINVH*: 100.200.140.206. This is the VIP where the domain-specific Administration Server is running, assigned to ethX:Y, available in *FINHOST1* to and *FINHOST2*.
  - The domain directory where the Administration Server is running on *FINHOST1* to is on shared storage and is mounted from *FINHOST2*

### 17.4.2 Performing the Failover

The following procedure explains how to fail over the Administration Server to a different node (*FINHOST2*) with the Administration Server still using the same Oracle WebLogic Server machine. (This machine is a logical machine, not a physical one.)

To fail over the Administration Server:

1. Stop the Administration Server.
2. Migrate the IP to the second node:
  - a. Run the following command as root on *FINHOST1* to (where X:Y is the current interface used by *FINADMINVH*):

```
FINHOST1> /sbin/ifconfig ethX:Y down
```

- b. Run the following command as root on *FINHOST2*:

```
FINHOST2> /sbin/ifconfig interface:index IP_Address netmask netmask
```

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 *FINHOST2*.

---

3. Update the routing tables with arping. For example, run the following command as root:

```
FINHOST2> /sbin/arping -b -A -c 3 -I eth0 100.200.140.206
```

4. Start the Administration Server on *FINHOST2* using the procedure in [Section 17.1.3](#).
5. Test access to the Administration Server on *FINHOST2*:

- a. Ensure that you can access the domain-specific Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control. For example, for the Oracle Fusion Financials domain, use these URLs:

```
- http://fininternal.mycompany.com:7777/console
```

```
- http://fininternal.mycompany.com:7777/em
```

- b. Repeat Step a for other domain by replacing the domain-specific URL.

---

**Note:** The Administration Server does not use Node Manager for failing over. After a manual failover, the machine name that appears in the Current Machine field in the Administration Console for the server is *FINHOST1*, and not the failover machine, *FINHOST2*. Since Node Manager does not monitor the Administration Server, the machine name that appears in the Current Machine field, is not relevant and you can ignore it.

---

## 17.5 Failing the Administration Server Back to FINHOST1

You also must ensure that you can fail back the Oracle WebLogic Server Administration Server, that is, stop it on *FINHOST2* and run it on *FINHOST1*. To do this, migrate *FINADMINVH* back to *FINHOST1* node.

To migrate *FINADMINVH*:

1. Run the following command as root from *FINHOST2* to shut down the network stack virtual interface:

```
FINHOST2> /sbin/ifconfig ethX:Y down
```

2. Run the following command as root from *FINHOST1* to restart the virtual interface:

```
FINHOST1> /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 *FINHOST1*.

---

3. Run the following command from *FINHOST1* to update the routing tables through arping:  

```
FINHOST1> /sbin/arping -b -A -c 3 -I ethZ 100.200.140.206
```
4. Start the Administration Server again on *FINHOST1* using the procedure in Step 3 in [Section 17.1.3](#).
5. Test access to the Administration Server on *FINHOST1*:
  - a. Ensure that you can access the domain-specific Oracle WebLogic Server Administration Console and Oracle Enterprise Manager Fusion Middleware Control. For example, for the Oracle Fusion Financials domain, use these URLs:
    - `http://fininternal.mycompany.com:7777/console`
    - `http://fininternal.mycompany.com:7777/em`
  - b. Repeat Step a for other domain by replacing the domain-specific URL.



---

## Setting Up Server Migration for an Enterprise Deployment

---

This chapter describes how to configure server migration according to enterprise deployment recommendations.

This chapter includes the following topic:

- [Section 18.1, "Prerequisite"](#)
- [Section 18.2, "Migrating Oracle Fusion Applications Domains"](#)

### 18.1 Prerequisite

Before migrating Oracle Fusion Applications domains, ensure you have completed the steps in [Section 16.1, "Enabling Virtual IPs on FINHOST1 and FINHOST2,"](#) [Section 16.2, "Setting the Listen Address for soa\\_server1,"](#) and [Section 16.3, "Setting the Listen Address for soa\\_server2"](#) for all Managed Servers needing to be migrated.

---

**Note:** This prerequisite does not apply to the Oracle Business Intelligence domain.

---

### 18.2 Migrating Oracle Fusion Applications Domains

The procedures in this section apply to these domains and applications:

- Oracle SOA Suite in the Oracle Fusion Financials domain
- Oracle SOA Suite and Oracle WebCenter Content: Imaging in the Oracle Fusion Common domain
- Oracle SOA Suite in the Oracle Business Intelligence domain
- Oracle SOA Suite in the Oracle Fusion Human Capital Management domain
- Oracle SOA Suite in the Oracle Fusion Supply Chain Management domain
- Oracle SOA Suite in the Oracle Fusion Projects domain
- Oracle SOA Suite in the Oracle Fusion Procurement domain

#### 18.2.1 About Configuring Server Migration

The procedures described in this chapter must be performed for various components of the enterprise deployment topology outlined in [Section 2.1, "Overview of Reference](#)

[Enterprise Deployment Topologies.](#)" Variables are used in this chapter to distinguish between component-specific items:

- *WLS\_SERVER1* and *WLS\_SERVER2* refer to the managed WebLogic servers for the enterprise deployment component
- *FINHOST1* and *FINHOST2* refer to the host machines for the enterprise deployment component
- *CLUSTER* refers to the cluster associated with the enterprise deployment component.

The values to be used to these variables are provided in the component-specific chapters in this guide.

In this enterprise topology, you must configure server migration for the *WLS\_SERVER1* and *WLS\_SERVER2* Managed Servers. The *WLS\_SERVER1* Managed Server is configured to restart on *FINHOST2* should a failure occur. The *WLS\_SERVER2* Managed Server is configured to restart on *FINHOST1* should a failure occur. For this configuration, the *WLS\_SERVER1* and *WLS\_SERVER2* servers listen on specific floating IP addresses that are failed over by WebLogic Server migration. Configuring server migration for the WLS Managed Servers consists of the following steps:

- Step 1: [Setting Up a User and Tablespace for the Server Migration Leasing Table](#)
- Step 2: [Creating a Multi-Data Source Using the Oracle WebLogic Server Administration Console](#)
- Step 3: [Editing Node Manager's Properties File](#)
- Step 4: [Setting Environment and Superuser Privileges for the wlsifconfig.sh Script](#)
- Step 5: [Configuring Server Migration Targets](#)
- Step 6: [Testing the Server Migration](#)

## 18.2.2 Setting Up a User and Tablespace for the Server Migration Leasing Table

The first step is to set up a user and tablespace for the server migration leasing table.

---

**Note:** If other servers in the same domain have already been configured with server migration, the same tablespace and data sources can be used. In that case, the data sources and multi-data source for database leasing do not need to be re-created, but they will have to be retargeted to the cluster being configured with server migration.

---

To set up a user and tablespace:

1. Create a tablespace called 'leasing'. For example, log on to SQL\*Plus as the sysdba user and run the following command:

```
SQL> create tablespace leasing logging datafile
'DB_HOME/oradata/orcl/leasing.dbf'
size 32m autoextend on next 32m maxsize 2048m extent management local;
```

2. Create a user named 'leasing' and assign to it the leasing tablespace:

```
SQL> create user leasing identified by welcomel;
SQL> grant create table to leasing;
SQL> grant create session to leasing;
SQL> alter user leasing default tablespace leasing;
```

```
SQL> alter user leasing quota unlimited on LEASING;
```

**3. Create the leasing table using the leasing.ddl script:**

- a. Copy the leasing.ddl file located in either the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/db/oracle/817` or the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/db/oracle/920` directory to your database node.
- b. Connect to the database as the leasing user.
- c. Run the leasing.ddl script in SQL\*Plus:

```
SQL> @Copy_Location/leasing.ddl;
```

### 18.2.3 Creating a Multi-Data Source Using the Oracle WebLogic Server Administration Console

The second step is to create a multi-data source for the leasing table from the Oracle WebLogic Server Administration Console. You create a data source to each of the Oracle RAC database instances during the process of setting up the multi-data source, both for these data sources and the global leasing multi-data source.

Please note the following considerations when creating a data source:

- Make sure that this is a non-XA data source.
- The names of the multi-data sources are in the format of `<MultiDS>-rac0`, `<MultiDS>-rac1`, and so on.
- Use Oracle's Driver (Thin) Version 9.0.1, 9.2.0, 10, 11.
- Use Supports Global Transactions, One-Phase Commit, and specify a service name for your database.
- Target these data sources to the cluster assigned to the enterprise deployment component (`CLUSTER`; see the component-specific chapters in this guide).

#### Creating a Multi-Data Source

To create a multi-data source:

1. In the Domain Structure window in the Oracle WebLogic Server Administration Console, click the **Data Sources** link.
2. Click **Lock & Edit**.
3. Select **Multi Data Source** from the **New** dropdown menu.  
The Create a New JDBC Multi Data Source page is displayed.
4. Enter `leasing` as the name.
5. Enter `jdbc/leasing` as the JNDI name.
6. Select **Failover** as algorithm (default).
7. Click **Next**.
8. Select the cluster assigned to the enterprise deployment component as the target.
9. Click **Next**.
10. Select **non-XA driver** (the default).
11. Click **Next**.

**12. Click Create a New Data Source.**

- 13.** Enter `leasing-rac0` as the name. Enter `jdbc/leasing-rac0` as the JNDI name. Enter `oracle` as the database type. For the driver type, select Oracle Driver (Thin) for Oracle RAC Service-Instance connections, Versions 10 and later.

---

**Note:** When creating the multi-data sources for the leasing table, enter names in the format of `<MultiDS>-rac0`, `<MultiDS>-rac1`, and so on.

---

**14. Click Next.**

**15. Deselect Supports Global Transactions.**

**16. Click Next.**

**17. Enter the following for your leasing schema:**

- **Service Name:** The service name of the database.
- **Database Name:** The Instance Name for the first instance of the Oracle RAC database.
- **Host Name:** The name of the node that is running the database. For the Oracle RAC database, specify the first instance's VIP name or the node name as the host name.
- **Port:** The port number for the database (1521).
- **Database User Name:** Enter `leasing`.
- **Password:** The leasing password.

**18. Click Next.**

**19. Click Test Configuration** and verify that the connection works.

**20. Click Next.**

**21.** Target the data source to the cluster assigned to the enterprise deployment component (*CLUSTER*).

**22. Click Finish.**

**23.** Click **Create a New Data Source** for the second instance of your Oracle RAC database, target it to the cluster assigned to the enterprise deployment component (*CLUSTER*), repeating the steps for the second instance of your Oracle RAC database.

**24.** Add `leasing -rac0` and `leasing -rac1` to your multi-data source.

**25.** Make sure the initial connection pool capacity of the data sources is set to 0 (zero). In the Datasources screen do the following:

- a. Select **Services**, then select **Datasources**.
- b. Click **Datasource Name**, then click the **Connection Pool** tab.
- c. Enter 0 (zero) in the **Initial Capacity** field.

**26. Click Save**, then click **Activate Changes**.

## 18.2.4 Editing Node Manager's Properties File

The third step is to edit Node Manager's properties file, which is located at:

```
ORACLE_BASE/products/fusionapps/wlserver_10.3/common/nodemanager/FINHOST1
```

```
ORACLE_BASE/products/fusionapps/wlserver_10.3/common/nodemanager/FINHOST2
```

This needs to be done for the node managers in both nodes where server migration is being configured. For example:

```
Interface=eth0
NetMask=255.255.255.0
UseMACBroadcast=true
```

- **Interface:** This property specifies the interface name for the floating IP (for example, eth0).  
  
Do not specify the sub-interface, such as eth0:1 or eth0:2. This interface is to be used without :0 or :1. Node Manager's scripts traverse the different :X-enabled IPs to determine which to add or remove. For example, the valid values in Linux environments are eth0, eth1, eth2, eth3, ethn, depending on the number of interfaces configured.
- **NetMask:** This property specifies the net mask for the interface for the floating IP. The net mask should be the same as the net mask on the interface; 255.255.255.0 is used as an example in this document.
- **UseMACBroadcast:** This property specifies whether or not to use a node's MAC address when sending ARP packets, that is, whether or not to use the -b flag in the arping command.

Verify in Node Manager's output (shell where Node Manager is started) that these properties are being used, or problems may arise during migration. You should see something like this in Node Manager's output:

```
...
StateCheckInterval=500
Interface=eth0
NetMask=255.255.255.0
...
```

---

**Note:** The steps below are not required if the server properties (start properties) have been properly set and Node Manager can start the servers remotely.

---

1. Set the following property in the `nodemanager.properties` file:
  - **StartScriptEnabled:** Set this property to 'true'. This is required for Node Manager to start the Managed Servers using start scripts.
2. Restart Node Manager on *FINHOST1* and *FINHOST2* by running the `startNodeManagerWrapper.sh` script, which is located in the `ORACLE_BASE/products/fusionapps/wlserver_10.3/common/nodemanager/FINHOST1` and `ORACLE_BASE/products/fusionapps/wlserver_10.3/common/nodemanager/FINHOST2` directories.

## 18.2.5 Setting Environment and Superuser Privileges for the `wlsifconfig.sh` Script

The fourth step is to set environment and superuser privileges for the `wlsifconfig.sh` script:

1. Ensure that your PATH is set with the environment variables in the terminal from where Node Manager is started, and that it includes these files:

**Table 18–1 Files Required for the PATH Environment Variable**

File	Located in this directory
wlsifconfig.sh	/u02/local/oracle/config/domains/ <i>FINHOSTn</i> /ManagedServer_Domain/bin/server_migration
wlscontrol.sh	ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin
nodemanager.domains	ORACLE_BASE/products/fusionapps/wlserver_10.3/common/nodemanager/ <i>FINHOSTn</i>

2. Grant sudo configuration for the wlsifconfig.sh script.
  - Configure sudo to work without a password prompt.
  - For security reasons, sudo should be restricted to the subset of commands required to run the wlsifconfig.sh script. For example, perform these steps to set the environment and superuser privileges for the wlsifconfig.sh script:
    - a. Grant sudo privilege to the WebLogic user ('oracle') with no password restriction, and grant execute privilege on the /sbin/ifconfig and /sbin/arping binaries.
    - b. Make sure the script is executable by the WebLogic user ('oracle'). The following is an example of an entry inside /etc/sudoers granting sudo execution privilege for oracle and also over ifconfig and arping:

```
oracle ALL=NOPASSWD: /sbin/ifconfig,/sbin/arping
```

---

**Note:** Ask the system administrator for the sudo and system rights as appropriate to this step.

---

## 18.2.6 Configuring Server Migration Targets

The fifth step is to configure server migration targets. You first assign all the available nodes for the cluster's members and then specify candidate machines (in order of preference) for each server that is configured with server migration. Follow these steps to configure cluster migration in a migration in a cluster:

1. Log in to the Oracle WebLogic Server Administration Console. For example, For example, <http://fininternal.mycompany.com:7777/console>.
2. In the Domain Structure window, expand **Environment** and select **Clusters**. The Summary of Clusters page is displayed.
3. Click the cluster for which you want to configure migration (**CLUSTER**) in the Name column of the table.
4. Click the **Migration** tab.
5. Click **Lock & Edit**.
6. In the **Available** field, select the machine to which to allow migration and click the right arrow. In this case, select *FINHOST1* and *FINHOST2*.

---

**Note:** When there are three (3) hosts, for example *FINHOST1*, *FINHOST2*, and *FINHOST3*, select all three hosts.

---

7. Select the data source to be used for automatic migration. In this case, select the leasing data source.
8. Click **Save**.
9. Click **Activate Changes**.
10. Set the candidate machines for server migration. You must perform this task for all of the Managed Servers as follows:

- a. In the Domain Structure window of the Oracle WebLogic Server Administration Console, expand **Environment** and select **Servers**.

**Tip:** Click **Customize this table** in the Summary of Servers page and move Current Machine from the Available window to the Chosen window to view the machine on which the server is running. This will be different from the configuration if the server gets migrated automatically.

- b. Select the server for which you want to configure migration.
- c. Click the **Migration** tab, and then click **Lock & Edit**.
- d. In the **Available** field, located in the Migration Configuration section, select the machines to which to allow migration and click the right arrow. For *WLS\_SERVER1*, select *FINHOST2*. For *WLS\_SERVER2*, select *FINHOST1*.

---

**Note:** If there are three (3) hosts (*FINHOST1*, *FINHOST2*, and *FINHOST3*) and three (3) servers (*WLS\_SERVER1*, *WLS\_SERVER2*, and *WLS\_SERVER3*), do the following:

In the **Configuration** section, select the machines to which you want to allow migration and click the right arrow. For *WLS\_SERVER1*, select *FINHOST2*; for *WLS\_SERVER2*, select *FINHOST3*; and for *WLS\_SERVER3*, select *FINHOST1*.

---

- e. Select **Automatic Server Migration Enabled**. This enables Node Manager to start a failed server on the target node automatically.
- f. Click **Save**.
- g. Click **Activate Changes**.
- h. Restart the administration server, node managers, and the servers for which server migration has been configured.

## 18.2.7 Testing the Server Migration

The sixth and final step is to test the server migration. Perform these steps to verify that server migration is working properly:

### From *FINHOST1*:

1. Stop the *WLS\_SERVER1* Managed Server. To do this, run this command:

```
FINHOST1> kill -9 pid
```

where *pid* specifies the process ID of the Managed Server. You can identify the pid in the node by running this command:

```
FINHOST1> ps -ef | grep WLS_SERVER1 | grep DomainName_SOACluster
```

2. Watch the Node Manager console. You should see a message indicating that *WLS\_SERVER1*'s floating IP has been disabled.
3. Wait for Node Manager to try a second restart of *WLS\_SERVER1*. It waits for a fence period of 30 seconds before trying this restart.
4. Once Node Manager restarts the server, stop it few times. Node Manager should now log a message indicating that the server will not be restarted again locally.

#### From FINHOST2:

1. Watch the local Node Manager console. After 30 seconds since the last try to restart *WLS\_SERVER1* on *FINHOST1*>, Node Manager on *FINHOST2*> should prompt that the floating IP for *WLS\_SERVER1* is being brought up and that the server is being restarted in this node.
2. As an example, for Oracle SOA Suite Managed Servers, access the soa-infra console in the same IP.

#### Verification from the Administration Console

Migration can also be verified in the Administration Console:

1. Log in to the Administration Console.
2. Click **Domain** on the left console.
3. Click the **Monitoring** tab and then the **Migration** subtab.

The Migration Status table, shown in [Figure 18–1](#), provides information on the status of the migration.

**Figure 18–1 Migration Status Screen in the Administration Console**

The screenshot displays the Oracle WebLogic Server Administration Console. The left sidebar shows the 'Domain Structure' with 'FinancialDomain' selected. The main area is titled 'Settings for FinancialDomain' and has tabs for 'Configuration', 'Monitoring', 'Control', 'Security', 'Web Service Security', and 'Notes'. The 'Monitoring' tab is active, and the 'Migration' subtab is selected. Below the subtabs, there is a table titled 'Migration Status' showing migration requests. The table has columns for Start Time, End Time, Status, Server, Machines Attempted, Machine Migrated From, Machine Migrated To, Cluster, and Cluster Master. The table shows four rows of migration data, with two in progress and two succeeded.

Start Time	End Time	Status	Server	Machines Attempted	Machine Migrated From	Machine Migrated To	Cluster	Cluster Master
2/17/12 7:19:40 PM CET		In Progress	soa_server1	FINHOST2	FINHOST1	FINHOST2	FIN_SOACluster	soa_server2
2/17/12 7:26:07 PM CET	2/17/12 7:31:41 PM CET	Succeeded	soa_server2	FINHOST1	FINHOST2	FINHOST1	FIN_SOACluster	soa_server1
2/23/12 8:38:13 AM CET	2/23/12 8:42:24 AM CET	Succeeded	soa_server1	FINHOST2	FINHOST1	FINHOST2	FIN_SOACluster	soa_server2
2/23/12 8:43:33 AM CET		In Progress	soa_server1	FINHOST1	FINHOST2	FINHOST1	FIN_SOACluster	soa_server2

Showing 1 to 4 of 4 Previous Next

---

**Note:** To complete server migration in a cluster, perform the same steps on the second, third, and so on, managed servers.

---



---

# Configuring Oracle Business Intelligence Applications

Configuration of Oracle Business Intelligence Applications is an extension of the existing Oracle Business Intelligence domain. This chapter describes how the different components of Oracle BI Applications can be installed and configured for high availability.

This chapter includes the following topics:

- [Section 19.1, "Introduction to Oracle BI Applications for Oracle Fusion Financials"](#)
- [Section 19.2, "Preparing for an Oracle BI Applications Installation"](#)
- [Section 19.3, "Performing Additional Configuration Tasks"](#)
- [Section 19.4, "Configuring Oracle HTTP Server for the Managed Server"](#)
- [Section 19.5, "Performing Additional Data Warehouse Administration Console Tasks"](#)
- [Section 19.6, "Validating Oracle BI Applications Components URLs"](#)

## 19.1 Introduction to Oracle BI Applications for Oracle Fusion Financials

Oracle Fusion Financials is seamlessly integrated with Oracle Business Intelligence Suite to address the full range of analytical requirements. The suite consists of two products, Oracle Transactional Business Intelligence and Oracle Business Intelligence Applications (Oracle BI Applications).

Oracle Transactional Business Intelligence delivers up-to-the minute analysis of a wide range of Oracle Fusion Financials subject areas, whereas Oracle BI Applications provides a more comprehensive historical perspective for Oracle Fusion Financials that is suited to deeper analytical assessments. The product suite is meant to work together to provide customers with the ability to adapt to the rapidly changing and diverse analytical needs required by the business. For example, a customer could use the Transactional Business Intelligence FIN Sales analysis area to view up to the minute pipeline analysis near key forecasting time periods; the projected forecast could then be further validated leveraging the FIN analysis area in Oracle BI Applications to see how this compares vs. previous time periods, sales people, customers, industries, etc. enabling sales management to make adjustments that deliver a more accurate overall forecast.

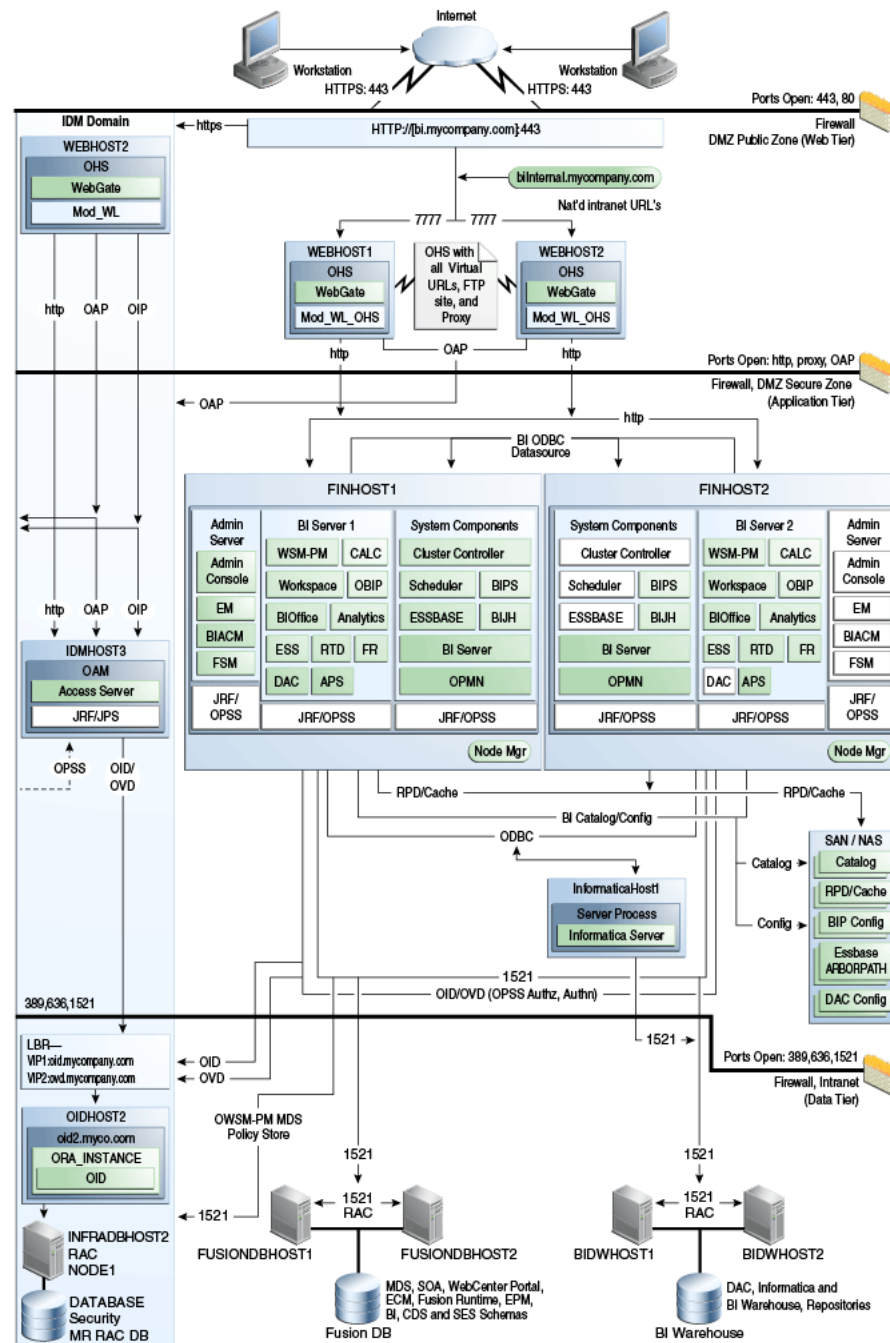
Oracle Transactional Business Intelligence is an integrated product of Oracle Fusion Applications. Oracle BI Applications is an optional product that you may choose to deploy. The ETL tier of Oracle BI Applications consists of the following components:

- a Data Warehouse database
- Informatica ETL suite
- Data Warehouse Administration Console (DAC)

The following sections provide more details about implementing these components of Oracle BI Applications for Oracle Fusion Applications.

### 19.1.1 Topology

[Figure 19–1](#) shows the topology that represents Oracle BI Applications implementation in the Oracle Fusion Applications environment.

**Figure 19–1 Data Warehouse for Oracle BI Applications**

## 19.2 Preparing for an Oracle BI Applications Installation

This section describes the following high-level tasks that are required to install Oracle BI Applications:

1. Create the Data Warehouse database.
2. Run the Repository Creation Utility (RCU) to create the Oracle BI Applications schemas for the Data Warehouse.
3. Install and configure Informatica PowerCenter.

For more information, see "Installing and Setting Up Informatica PowerCenter" in *Oracle Fusion Middleware Configuration Guide for Oracle Business Intelligence Applications*.

4. Extend the Oracle Business Intelligence domain by deploying Oracle BI Applications Configuration Manager, Oracle Fusion Functional Setup Manager, and Oracle Business Intelligence Data Warehouse Administration Console (DAC).
5. Perform any necessary post-installation steps to complete the Oracle BI Applications setup.

## 19.2.1 Creating Databases for Oracle Business Intelligence Applications Components

Before you install Oracle BI Applications, the Data Warehouse Administration Console (DAC), and Informatica PowerCenter, create an Oracle RAC database on *BIDWHOST1* and *BIDWHOST2* to hold the following:

- DAC Repository
- Informatica Domain Configuration Database
- Informatica Repository
- Oracle Business Analytics Warehouse

For information, see the following:

- [Section 4.2, "Setting Up the Database."](#)
- "Pre-installation and Pre-deployment Requirements for Oracle BI Applications" in *Oracle Fusion Middleware Configuration Guide for Oracle Business Intelligence Applications*.

## 19.2.2 Running Oracle BI Applications RCU to Create the Oracle BI Applications Schemas for the Data Warehouse

You must run the Oracle BI Applications Repository Creation Utility (RCU) to create the following Oracle BI Applications schemas:

- Oracle Data Warehouse Administration Console
- Oracle Business Analytics Warehouse

---

**Note:** Before running Oracle BI Applications RCU, you must copy the export dump files from the *RCU\_HOME/rcu/integration/biapps/schema* directory to the *BIDWHOST1* and *BIDWHOST2* Oracle RAC database nodes. These dump files will be required when entering values in the Custom Variables screen ([Figure 19–5](#)). The directory should have read/write access since logs are written to it during the import.

---

For more information, see "Create the Oracle BI Applications Schemas Using RCU" in *Oracle Fusion Middleware Configuration Guide for Oracle Business Intelligence Applications*.

To run the Oracle BI Applications RCU:

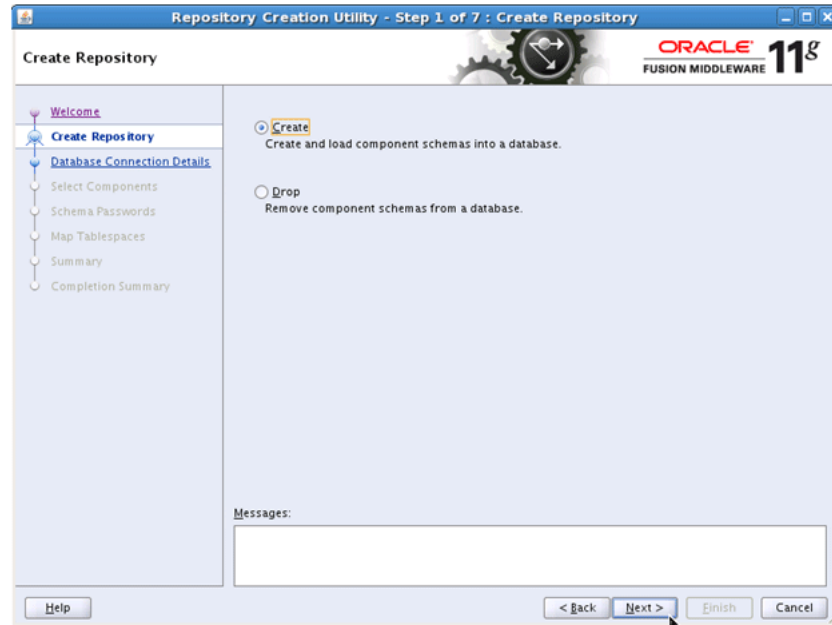
1. Unzip the *ORACLE\_BASE/repository/installers/biapps\_rcu/linux/rcuHomeBIApps.zip* file in the RCU home directory, and then start RCU from the bin directory in the RCU home directory:

```
cd RCU_HOME/bin
```

./rcu

2. In the Welcome screen (if displayed), click **Next**.
3. In the Create Repository screen, shown in [Figure 19-2](#), select **Create** to load component schemas into a database. Click **Next**.

**Figure 19-2 Create Repository Screen**



4. In the Database Connection Details screen, shown in [Figure 19-3](#), enter connect information for your database:
  - **Database Type:** Select **Oracle Database** from the dropdown list
  - **Host Name:** Specify the name of the node on which the database resides. For the Oracle RAC database, specify the VIP name or one of the node names as the host name: `BIDWHOST1-VIP`
  - **Port:** Specify the listen port number for the database
  - **Service Name:** Specify the service name of the database (`bidw.mycompany.com`).
  - **Username:** Specify the name of the user with DBA or SYSDBA privileges: `SYS`.
  - **Password:** Enter the password for the SYS user.
  - **Role:** Select the database user's role from the dropdown list: `SYSDBA` (required by the SYS user).

Click **Next**.

**Figure 19–3 Database Connection Details Screen**

Repository Creation Utility - Step 2 of 7: Database Connection Details

Database Connection Details

Oracle 11g FUSION MIDDLEWARE

Database Type: Oracle Database

Host Name: bidwhost1-vip  
For RAC database, specify VIP name or one of the Node name as Host name.

Port: 1521

Service Name: bidw.mycompany.com

Username: sys  
User with DBA or SYSDBA privileges. Example: sys

Password: ••••••••

Role: SYSDBA  
One or more components may require SYSDBA role for the operation to succeed.

Messages:

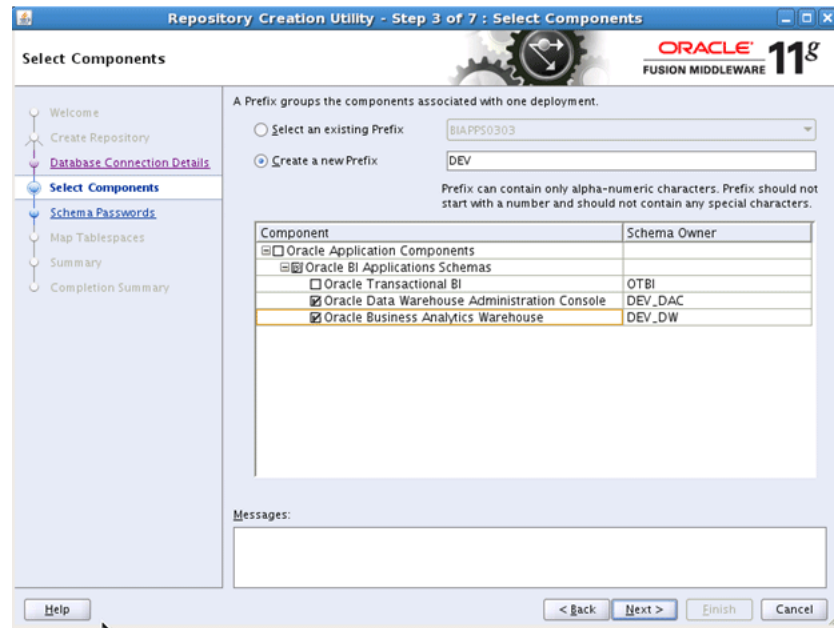
Help < Back Next > Finish Cancel

5. In the Select Components screen, shown in [Figure 19–4](#), do the following:
  - a. Select **Create a new Prefix**, and enter a prefix to use for the database schemas, for example DEV or PROD. You can specify up to six characters as a prefix. Prefixes are used to create logical groupings of multiple repositories in a database. For more information, see *Oracle Fusion Middleware Repository Creation Utility User's Guide*.

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

  - b. First select **Oracle Application Components** and then select the following:
    - Oracle BI Applications Schemas
      - Oracle Data Warehouse Administration Console
      - Oracle Business Analytics Warehouse

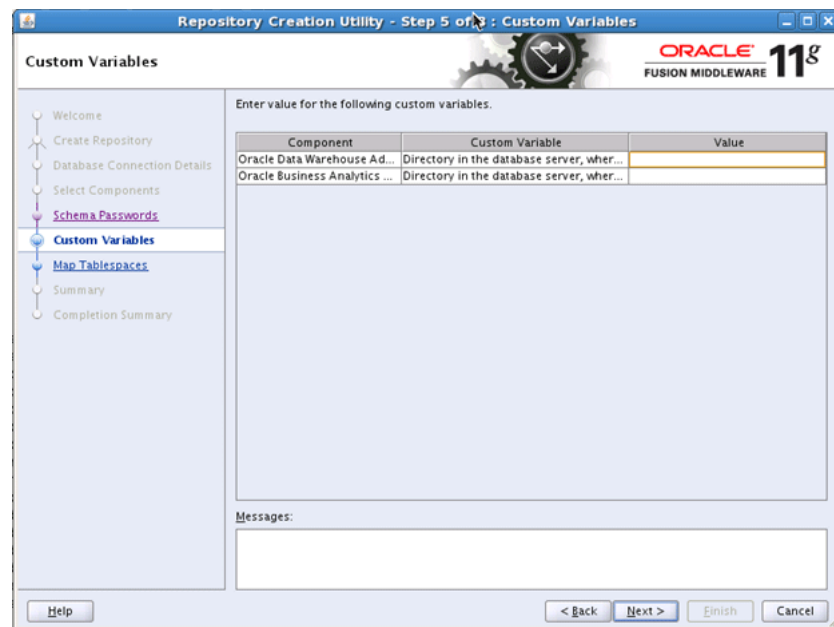
Click **Next**.

**Figure 19–4 Select Components Screen**

6. In the Schema Passwords screen, enter passwords for the main and additional (auxiliary) schema users, and click **Next**.

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

7. In the Custom Variables screen, shown in [Figure 19–5](#), enter the required values.

**Figure 19–5 Custom Variables Screen**

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

9. In the Summary screen, click **Create**.
10. In the Completion Summary screen, click **Close**.

### 19.2.3 Installing and Configuring Informatica PowerCenter Services

Informatica is a third-party component that is required for Oracle BI Applications implementation. *INFA\_HOME*, which refers to the user-specified Informatica installation directory on the machine that hosts Informatica PowerCenter Services, must be on shared storage that is accessible from *FINHOST1/* and *FINHOST2/* where DAC Server will be configured.

Download the Informatica PowerCenter software. For information about how to do so, see "Installing and Setting Up Informatica PowerCenter" in *Oracle Fusion Middleware Configuration Guide for Oracle Business Intelligence Applications*. During installation of Informatica PowerCenter, use the Oracle RAC database installed in [Section 19.2.1, "Creating Databases for Oracle Business Intelligence Applications Components"](#) when prompted.

### 19.2.4 Extending the Oracle Business Intelligence Domain by Deploying Oracle BI Applications Configuration Manager, Functional Setup Manager, and DAC

This section includes the following topics:

- [How to Configure DAC, Oracle BI Applications Configuration Manager, and Functional Setup Manager](#)
- [Configuring Data Warehouse Administration Console for High Availability](#)

---

---

**Note:** The DAC, Oracle BI Applications Configuration Manager, and Oracle Fusion Functional Setup Manager, configurations are an extension of the existing Oracle Business Intelligence domain. These procedures assume that Oracle Business Intelligence has been installed and configured during the Oracle Fusion Applications Provisioning process.

---

---

#### 19.2.4.1 How to Configure DAC, Oracle BI Applications Configuration Manager, and Functional Setup Manager

The DAC, Oracle BI Applications Configuration Manager, and Functional Setup Manager configuration is an extension of the existing Oracle Business Intelligence domain. In this extension, the Oracle BI Applications Configuration Manager, and Functional Setup Manager components are administration components and are targeted to the Administration Server. DAC will be targeted to the Oracle Business Intelligence Managed Server.

To extend the domain:

1. Run the WebLogic Scripting Tool (WLST) script, *ORACLE\_BASE/products/fusionapps/bi/dwtools/scripts/install\_dwtools.py* from *FINHOST1/*. A sample script is shown in [Example 19-1](#).

##### **Example 19-1** Running the WLST Script

```
ORACLE_BASE/products/fusionapps/bi/common/bin/wlst.sh install_dwtools.py
'DOMAIN_HOME'
'INFORMATICA_SERVER_HOME'
'INFORMATICA_DOMAIN_FILE'
```

```
'DW_DB_URL' 'DW_DB_SCHEMA'
'MDS_DB_URL' 'MDS_DB_SCHEMA'
'DAC_DB_URL' 'DAC_SCHEMA'
'DAC_TARGET'
```

where:

- *DOMAIN\_HOME* is the path to the Administration Server Domain Home
- *INFORMATICA\_SERVER\_HOME* is the path to the Informatica Server Home
- *INFORMATICA DOMAIN FILE* is the path to the Informatica domains.infa file location

- *DW\_DB\_URL* is the string; for example,

```
'jdbc:oracle:thin:@(DESCRIPTION=
(ADDRESS_LIST=(LOAD_BALANCE=on)
(ADDRESS=(PROTOCOL=TCP)
(HOST=BIDWHOST1)(PORT=1521)) (ADDRESS=
(PROTOCOL=TCP) (HOST=BIDWHOST2)
(PORT=1521))) (CONNECT_DATA=
(SERVICE_NAME=bidw.mycompany.com))) '
```

- *DW\_DB\_SCHEMA* is the Data Warehouse schema; for example, *prefix\_DW*

- *MDS\_DB\_URL* is the string; for example,

```
'jdbc:oracle:thin:@(DESCRIPTION=
(ADDRESS_LIST=(LOAD_BALANCE=on)
(ADDRESS=(PROTOCOL=TCP)
(HOST=FUSIONDBHOST1)(PORT=1521))
(ADDRESS=(PROTOCOL=TCP)
(HOST=FUSIONDBHOST2)(PORT=1521)))
(CONNECT_DATA=
(SERVICE_NAME=fin.mycompany.com))) '
```

- *MDS\_DB\_SCHEMA* is the MDS schema; for example, *prefix\_MDS*

- *DAC\_DB\_URL* is the string; for example,

```
'jdbc:oracle:thin:@(DESCRIPTION=
(ADDRESS_LIST=(LOAD_BALANCE=on)
(ADDRESS=(PROTOCOL=TCP)
(HOST=BIDWHOST1)(PORT=1521)) (ADDRESS=
(PROTOCOL=TCP) (HOST=BIDWHOST2)
(PORT=1521))) (CONNECT_DATA=
(SERVICE_NAME=bidw.mycompany.com))) '
```

- *DAC\_SCHEMA* is the DAC schema; for example, *prefix\_DAC*

---

**Note:** When prompted, enter the password for each of the following schemas:

- *prefix\_DW*
  - *prefix\_MDS*
  - *prefix\_DAC*
- 

- *DAC\_TARGET* should be set to the Managed Server name (*bi\_server1*) for an enterprise installation or *AdminServer* for a simple installation.

---

---

**Note:** You must restart the Administration Server for this configuration to take effect.

---

---

2. Run the following Oracle WebLogic Scripting Tool (WLST) script from *FINHOST1*:

```
ORACLE_BASE/products/fusionapps/bi/dac/scripts/copyDACDomainFiles.py
```

For example:

```
ORACLE_BASE/products/fusionapps/bi/common/bin/wlst.sh copyDACDomainFiles.py
'ORACLE_HOME' 'DOMAIN_HOME'
```

where

- *ORACLE\_HOME* is the path to Oracle home. For example, *ORACLE\_BASE/products/fusionapps/bi*.
- *DOMAIN\_HOME* is the path to the Managed Server domain home. For example, */u02/local/oracle/config/domains/FINHOST1/BIDomain*.

3. Restart the Administrative Server and all Managed Servers.

4. Run the following WLST script on *FINHOST1*:

```
ORACLE_BASE/products/fusionapps/bi/dwtools/scripts/configure_dwtools.py
```

For example:

```
ORACLE_BASE/products/fusionapps/bi/common/bin/wlst.sh configure_dwtools.py
'WEBLOGIC_ADMINISTRATOR'
'WEBLOGIC_ADMIN_SERVER_HOST'
'WEBLOGIC_ADMIN_SERVER_PORT'
```

You will be prompted for the WebLogic Administrator password.

5. Run the following WLST script on *FINHOST1*:

```
ORACLE_BASE/products/fusionapps/bi/dwtools/scripts/configure_rpd.py
```

For example:

```
$ cd ORACLE_BASE/products/fusionapps/bi/dwtools/scripts/
$ ORACLE_BASE/products/fusionapps/bi/common/bin/wlst.sh configure_rpd.py
'DOMAIN_HOME'
'DW_DB_URL'
'DW_DB_SCHEMA'
'MASTER_BI_INSTANCE_HOME'
'WEBLOGIC_ADMIN_SERVER_HOST'
'WEBLOGIC_ADMIN_SERVER_PORT'
'WEBLOGIC_ADMINISTRATOR'
```

where

- *DOMAIN\_HOME* is the path to the Managed Server domain home. For example, */u02/local/oracle/config/domains/FINHOST1/BIDomain*.
- *DW\_DB\_URL* is the string. For example,  

```
'jdbc:oracle:thin:@(DESCRIPTION=
(ADDRESS_LIST=(LOAD_BALANCE=on)
(ADDRESS=(PROTOCOL=TCP)
(HOST=BIDWHOST1)(PORT=1521)) (ADDRESS=
(PROTOCOL=TCP) (HOST=BIDWHOST2)
```

```
(PORT=1521)) (CONNECT_DATA=
(SERVICE_NAME=bidw.mycompany.com))) '
```

- *DW\_DB\_SCHEMA* is the Data Warehouse schema. For example, *prefix\_DW*.
  - *MASTER\_BI\_INSTANCE\_HOME* is the path to the Master BI Server Instance home. For example, */u02/local/oracle/config/BIInstance*.
  - *WEBLOGIC\_ADMIN\_SERVER\_HOST* is the Oracle WebLogic Server Administration host. For example, *FINHOST1*.
  - *WEBLOGIC\_ADMIN\_SERVER\_PORT* is the Oracle WebLogic Server Administration Console Port. For example, 10201.
  - *WEBLOGIC\_ADMINISTRATOR* is the Oracle WebLogic Server Administrator.
6. On all nodes where DAC Server can run, update the */u02/local/oracle/config/domains/FINHOST1/BIDomain/bin/setDomainEnv.sh* script to include the following:
- ```
# Set Informatica Environment for DAC Server
. ${DOMAIN_HOME}/config/dac/dac_env.sh
```
7. For the changes to take effect, restart the Managed Servers and the System Components:
- a. On the Summary of Servers page, select the **Control** tab.
 - b. Select **bi_server1** and **bi_server2** in the table and then click **Shutdown**.
 - c. After the servers have shut down, select **bi_server1** and **bi_server2** in the table and then click **Start**.
 - d. Run the following commands to restart the Oracle Business Intelligence system components:

```
$ cd /u02/local/oracle/config/BIInstancen/bin
$ ./opmnctl stopall
$ ./opmnctl startall
```
8. Validate the Oracle BI Applications components:
- a. Log in to the Administration Server console (<http://biinternal.mycompany.com:7777/console>) and check the health and status of the Data Warehouse Administration Console Server (DACServer).
 - b. Validate the following DAC URL: <http://BIVH1:10217/DACServer>.
 - c. Check to ensure that the following files have been created:

```
ORACLE_BASE/config/domains/FINHOST1/BIDomain/dac/conf-shared/
server.properties

ORACLE_BASE/config/domains/FINHOST1/BIDomain/dac/
conf-shared/security/repository/cwallet.sso
```
 - d. Log in to the database with the DAC schema user name and password and type the following SQL query:

```
SELECT * FROM W_ETL_REPOS WHERE ROW_WID='DACServerURL';
```
 - e. Check the **VALUE** column of the result.
- The default value before configuration is <http://FINHOST1:10217/DACServer>. The hostname and port will be updated in Step 1 in [Section 19.2.4.2](#).

19.2.4.2 Configuring Data Warehouse Administration Console for High Availability

The Data Warehouse Administration Console (DAC) Server is a singleton: only one active Oracle DAC Server is used at any given time. The Oracle WebLogic Server Migration feature is used to protect Oracle DAC server from failures. The Oracle WebLogic Managed Server in which Oracle DAC server runs is listening on a virtual IP that gets migrated to another node when the failure occurs.

For more information on server-migration features, see [Chapter 18, "Setting Up Server Migration for an Enterprise Deployment."](#)

1. Run the following WLST script to move the DAC configuration files to a new shared location:

```
ORACLE_BASE/products/fusionapps/bi/dac/scripts/moveDACConfigLocation.py
```

For example:

```
ORACLE_BASE/products/fusionapps/bi/common/bin/wlst.sh  
moveDACConfigLocation.py 'DOMAIN_HOME' 'DAC_SHARED_LOCATION'
```

where

- *DOMAIN_HOME* is the path to the Administration Server domain home.
 - *DAC_SHARED_LOCATION* is the DAC shared location. For example, *ORACLE_BASE/config/BIShared/dac*.
2. Restart the Administration Server and Managed Servers (ensure that Node Manager is up and running):
 - a. Log in to the Oracle WebLogic Server Administration Console (<http://biinternal.mycompany.com:7777/console>).
 - b. In the Summary of Servers screen, select the **Control** tab.
 - c. Select **AdminServer**, **bi_server1** and **bi_server2** in the table and then click **Shutdown**.
 - d. Restart the AdminServer, bi_server1, and bi_server2 Managed Servers.
 - e. Restart the Oracle Business Intelligence system components:

```
$ cd /u02/local/oracle/config/BIInstances/bin  
$ ./opmnctl stopall  
$ ./opmnctl startall
```

19.3 Performing Additional Configuration Tasks

For more information, see the following sections in *Oracle Fusion Middleware Configuration Guide for Oracle Business Intelligence Applications*:

- "Roadmap for Setting Up Oracle Business Intelligence Applications"
- "Configure SSO for Configuration Manager and Functional Setup Manager"

19.4 Configuring Oracle HTTP Server for the Managed Server

To enable Oracle HTTP Server to route to the Data Warehouse Component Managed Server, you must set the WebLogicHost parameter.

To set the WebLogicHost parameter:

1. Add the following line to the Oracle HTTP Server's

/u01/oracle/config/CommonDomain_
webtiern/config/OHS/ohs1/moduleconf/FusionVirtualHost_bi.conf file on
WEBHOST1 and *WEBHOST2*:

```
RedirectMatch 301 ^/DACServer$ /DACServer/
```

```
RedirectMatch 301 ^/biacm$ /biacm/
```

```
# DAC Server
<LocationMatch ^/DACServer/>
  SetHandler weblogic-handler
  WebLogicHost BIVH1
  WebLogicPort 10217
</LocationMatch>

## Context roots for application biacm
<LocationMatch ^/biacm/>
  SetHandler weblogic-handler
  WebLogicCluster BIADMINVH:10201
</LocationMatch>

## Context roots for application fsm
<LocationMatch /setup >
  SetHandler weblogic-handler
  WebLogicCluster BIADMINVH:10201
</LocationMatch>
```

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

```
WEBHOST1> ORACLE_BASE/config/CommonDomain_webtier/bin/opmnctl restartproc
ias-component=ohs1
```

```
WEBHOST2> ORACLE_BASE/config/CommonDomain_webtier1/bin/opmnctl restartproc
ias-component=ohs1
```

19.5 Performing Additional Data Warehouse Administration Console Tasks

Perform the following additional tasks:

1. Set the correct DACServer URL in DAC Repository using the SQL statement shown in [Example 19-2](#).

The DACServerURL should be set to point to the load balancer virtual server.

Example 19-2 Set the DACServer URL

```
SQL>
UPDATE "prefix_DAC"."W_ETL_REPOS" SET VALUE =
'http://biinternal.mycompany.com:7777/DACServer'
WHERE ROW_WID = 'DACServerURL';
SQL>
commit;
```

2. From the *ORACLE_BASE/config/domains/FINHOST1/BIDomain/dac* directory, start the DAC Client using `startclient.sh` and try to configure a new connection to validate the DAC Server setup. For more information, see "Logging into DAC for the First Time as an Administrator" in *Oracle Fusion Middleware User's Guide for Oracle Business Intelligence Data Warehouse Administration Console*.

19.6 Validating Oracle BI Applications Components URLs

To validate, access the following URLs:

- <http://biinternal.mycompany.com:7777/biacm> to verify the status BI Applications Configuration Manager
- <http://biinternal.mycompany.com:7777/setup/faces/TaskListManagerTop> to verify the status of Oracle Fusion Functional Setup Manager

Also, ensure that clicking on the "Perform Functional Configurations" link from Oracle BI Applications Configuration Manager launches Functional Setup Manager.

- <http://biinternal.mycompany.com:7777/DACServer> to verify the status of the DAC Server

Verify URLs to ensure that appropriate routing is working from the HTTP Server to the DAC Server.

To verify, access <http://WEBHOST1:10621/DACServer> and verify the appropriate functionality.

Managing the Topology

This chapter describes some operations that you can perform after you have set up the topology. These operations include monitoring, scaling, and backing up.

This chapter includes the following topics:

- [Section 20.1, "Scaling the Topology for Additional Nodes"](#)
- [Section 20.2, "Performing Backups and Recoveries"](#)
- [Section 20.3, "Monitoring the Topology"](#)
- [Section 20.4, "Migrating from a Test Environment to a Production Environment"](#)
- [Section 20.5, "Configuring Log File Rotation"](#)
- [Section 20.6, "Patching the Topology"](#)
- [Section 20.7, "Auditing"](#)
- [Section 20.8, "Troubleshooting"](#)

Note: For Oracle WebCenter Content scale out only, use the procedure described in [Section 10.4, "Scaling Out Oracle WebCenter Content."](#)

20.1 Scaling the Topology for Additional Nodes

You can scale out and or scale up the enterprise topology. When you scale up the topology, you add new Managed Servers to nodes that are already running on one or more Managed Servers. When you scale out the topology, you add new Managed Servers to new nodes.

This section includes the topics:

- [Section 20.1.1, "Scaling Out the Topology \(Adding Managed Servers to a New Node\) for Oracle ADF Server"](#)
- [Section 20.1.2, "Scaling Up the Topology \(Adding Managed Servers to an Existing Node\) for Oracle ADF Server"](#)
- [Section 20.1.3, "Scaling Out the Topology \(Adding Managed Servers to a New Node\) for Oracle SOA Suite Server"](#)
- [Section 20.1.4, "Scaling Up the Topology \(Adding Managed Servers to an Existing Node\) for Oracle SOA Suite Server"](#)
- [Section 20.1.5, "Scaling Out the Topology \(Adding Managed Servers to a New Node\) for Oracle Business Intelligence"](#)

- [Section 20.1.6, "Scaling Up the Topology for Oracle Business Intelligence"](#)

20.1.1 Scaling Out the Topology (Adding Managed Servers to a New Node) for Oracle ADF Server

When scaling out the topology, you add new Managed Servers configured to new nodes.

Note: The steps provided in this section also can be used to scale out additional hosts, such as *FINHOST4*, *FINHOST5*, and so on.

20.1.1.1 Prerequisites for Scaling Out the Topology for Oracle ADF Server

Before you begin, ensure the following:

- Node Manager has been started in the Secure Sockets Layer (SSL) mode by following the instructions in [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"](#)
- You are starting with a clean machine if it is the first time it is being used for a scale out
- The `/etc/hosts` file has proper entries. To verify, ping this machine with the fully qualified name of the machine
- The user created on *FINHOST3* should be the same as the user on *FINHOST1*
- The directory structure `/u01/oracle` is mounted to same shared file system as *FINHOST1*
- The directory structure `/u02/local/oracle/config` on *FINHOST3* has been created
- The initial Oracle Fusion Financials deployment on *FINHOST1* has already been done and verified by provisioning

20.1.1.2 Adding a New Machine in the Oracle WebLogic Server Console

To add a new machine:

1. Log in to the Administration Server:
`http://commoninternal.mycompany.com:7777/console.`
2. Navigate to **CommonDomain > Environment > Machines**.
LocalMachine is located in the right-hand pane.
3. In the left-hand pane, click **Lock & Edit**.
4. In the right-hand pane, first click **New** to add the remote machine, and then specify the following:
 - Name - enter *FINHOST3*
 - Machine operating system - Unix
5. Click **Next**.
6. In the window that opens, set the following attributes:
 - Type - SSL
 - Listen Address - `<FINHOST3>`

Note: The "localhost" default value here is wrong.

- Listen port - 5556
7. Click **Finish** and activate the changes.

Note: If you get an error when activating the changes, see [Section 20.8.18, "Administration Console Redirects from Internal URL to Container URL after Activation"](#) for the temporary solution.

20.1.1.3 Packing and Unpacking the Managed Server Domain Home

Since the *FINHOST1* domain directory file system is also available from *FINHOST3*, both the pack and unpack commands can be executed from the *FINHOST3*.

To pack and unpack the Managed Server domain home:

1. Change directory to *ORACLE_BASE*/products/fusionapps/oracle_common/common/bin.
2. Run the pack command. For CommonDomain, for example:


```
FINHOST3> ./pack.sh -managed=true -domain=ORACLE_BASE/config/domains/  
FINHOST1/CommonDomain -template=ORACLE_BASE/user_templates/  
CommonDomain_managed.jar -template_name="Common_Managed_Server_Domain"
```
3. Ensure that */u02/local/oracle/config/domains/FINHOST3/CommonDomain* is empty, and then run the unpack command:


```
FINHOST3> ./unpack.sh -domain=/u02/local/oracle/config/domains/  
FINHOST3/CommonDomain -template=ORACLE_BASE/user_templates/  
CommonDomain_managed.jar
```

Here, *ORACLE_BASE* is shared, and */u02/local* is local to *FINHOST3*.

20.1.1.4 Cloning Managed Servers and Assigning Them to FINHOST3

To add a Managed Server and assign it to *FINHOST3*:

1. Log in to the Administration Server:
`http://commoninternal.mycompany.com:7777/console.`
2. Navigate to **CommonDomain > Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the *Managed_Server* checkbox (for example, **HomePageServer_1**) and then click **Clone**.
5. Specify the following Server Identity attributes:
 - Server Name - HomePageServer_3

Note: To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to "_3"

- Server Listen Address - <FINHOST3>
- Server Listen Port - leave "as is"

Note: For Oracle SOA Suite server, add a port value that is different than the `soa_server1` server value. This will help in server migration.

6. Click **OK**.

You now should see the newly cloned server, `HomePageServer_3`.

7. Click **HomePageServer_3** and change the following attributes:

- Machine - <FINHOST3>
- Cluster Name - accept the default, `HomePageCluster`

Note: Ensure that this cluster name is the same as the cluster name of the original Managed Server.

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

9. From the **Name** column, click the **HomePageServer_3** scaled-out server link.

10. Click **Lock & Edit**, and then select the **Configuration** tab.

11. Select the **Keystores** tab, and then ensure that the keystores value is **Custom Identity and Custom Trust**.

12. Do the following:

- a. Change the Custom Identity Keystore path to point to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/FINHOST3_fusion_identity.jks` file.
- b. Leave the Custom Identity Keystore type blank.
- c. Change the Custom Identity Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
- d. Re-enter the Confirm Custom Identity Keystore Passphrase.
- e. Ensure that the Confirm Custom Trust Keystore path is pointing to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks` file.
- f. Leave the Custom Trust Keystore type blank.
- g. Change the Custom Trust Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
- h. Re-enter the Custom Trust Keystore Passphrase.
- i. Click **Save**.

13. Select the **SSL** tab.

- a. Make sure that Identity and Trust Locations is set to **Keystores**.
- b. Change the Private Key Alias to `FINHOST3_fusion`.

- c. Change the Private Key Passphrase to the *keypassword*, as described in the second bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
- d. Re-enter the *keypassword* from Step c for the Confirm Private Key Passphrase.
- e. Click **Save**.

14. Select the **Server Start tab.**

Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

```
-DJDBCProgramName\=DS/CommonDmain/HomePageServer_3
-Dserver.group\=HomePageCluster
```

Click **Save**.

15. Select the **Logging tab, and then select the **HTTP** tab.**

16. Do the following:

- a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.
- b. Change the rotation type to **By Time**.
- c. Leave the **Limit number of retained files** option unchecked.
- d. Leave the **Rotate log file on startup** option unchecked.
- e. Click **Save**.
- f. Expand **Advanced**.
- g. Change the format to **Extended**.
- h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri
sc-status sc(X-ORACLE-DMS-ECID)
cs(ECID-Context) cs(Proxy-Remote-User)
cs(Proxy-Client-IP)
```

- i. Click **Save**.

17. Click **Activate Changes.**

18. Repeat Steps 2 to 17 for all the newly cloned Managed Servers on this domain.

19. Set the following environment variable on *FINHOST3*:

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/
products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks"
```

20. Restart the domain's Administration Server on *FINHOST3*:

```
FINHOST3> ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin/wlst.sh

FINHOST3> nmConnect(username='<username>', password='<password>',
domainName='CommonDomain', host='FINHOST1',port='5556',
nmType='ssl', domainDir='ORACLE_BASE/config/domains/FINHOST1/CommonDomain')

FINHOST3> nmStart('AdminServer')
```

Note: The *username* and *password* used in the `nmConnect` are the Node Manager credentials (username and password) specified when creating the provisioning response file. This is shown in [Figure 5–3 in "Using the Provisioning Process to Install Components for an Enterprise Deployment"](#).

21. Run the newly created Managed Servers:

- a. Log in to the Administration Server:
`http://commoninternal.mycompany.com:7777/console.`
- b. Navigate to **CommonDomain > Environment > Servers > Control**.
- c. Check the newly created Managed Servers and click **Start**.
- d. Navigate to **CommonDomain > Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.

20.1.1.5 Validating the System

You should verify URLs to ensure that the appropriate routing and failover are working.

To verify the URLs:

1. Log in to the CommonDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on the `FINHOST1` while the Managed Servers on `FINHOST3` while they are running.
2. Access the following URL to verify that routing and failover are functioning properly. (Ensure the log in prompt is visible.)
`https://commonexternal.mycompany.com/homePage/faces/AtkHomePageWelcome`
3. Log in to the CommonDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on `FINHOST3`.
4. Start the Managed Servers on `FINHOST1`.
5. Repeat Step 2. (Ensure the log in prompt is visible.)
6. Start all the Managed Servers on `FINHOST3` and verify that they are running on `FINHOST1` and `FINHOST3`.

20.1.2 Scaling Up the Topology (Adding Managed Servers to an Existing Node) for Oracle ADF Server

Before performing the procedures in this section, ensure that CommonDomain and its Managed Servers are running.

20.1.2.1 Cloning Managed Servers and Assigning Them to FINHOST3

To add a Managed Server and assign it to `FINHOST3`:

1. Log in to the Administration Server:
`http://commoninternal.mycompany.com:7777/console.`
2. Navigate to **CommonDomain > Environment > Servers**.
3. Switch to **Lock & Edit** mode.

4. Select the *Managed_Server* checkbox (for example, **HomePageServer_1**) and then click **Clone**.
5. Specify the following Server Identity attributes:
 - Server Name - HomePageServer_4

Note: To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to "_4".

- Server Listen Address - <FINHOST3>
 - Server Listen Port - leave "Give an unused port on the machine FINHOST3"
6. Click **OK**.
 7. Navigate back to **CommonDomain > Environment > Servers**. You now should see the newly cloned server, HomePageServer_4.
 8. Click **HomePageServer_4** and change the following attributes:
 - Machine - <FINHOST3>
 - Cluster Name - accept the default, HomePageCluster

Note: Ensure that this cluster name is the same as the cluster name of the original Managed Server.

9. From **HomePageServer_4**, click **Advanced** and then select the **WebLogic Plug-In Enabled** checkbox.
10. Click **Save**.
11. Run the newly created Managed Server:
 - a. Navigate to **CommonDomain > Environment**.
 - b. From the **Navigation** pane on the Oracle WebLogic Server console, select **Activate Changes**.
 - c. Navigate to **CommonDomain > Environment > Servers > Control**.
 - d. Check the newly created Managed Server and click **Start**.
 - e. Navigate to **CommonDomain > Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.
12. Log in to the Administration Server once again (<http://commoninternal.mycompany.com:7777/console>) and verify that all the Managed Servers, including scaled-up servers, are running.
13. Select the **Server Start** tab.

Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

```
-DJDBCProgramName\=DS/CommonDmain/HomePageServer_4
-Dserver.group\=HomePageCluster
```

Click **Save**.

14. Select the **Logging** tab, and then select the **HTTP** tab.
15. Do the following:
 - a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.
 - b. Change the rotation type to **By Time**.
 - c. Leave the **Limit number of retained files** option unchecked.
 - d. Leave the **Rotate log file on startup** option unchecked.
 - e. Click **Save**.
 - f. Expand **Advanced**.
 - g. Change the format to **Extended**.
 - h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri
sc-status sc(X-ORACLE-DMS-ECID)
cs(ECID-Context) cs(Proxy-Remote-User)
cs(Proxy-Client-IP)
```
 - i. Click **Save**.
16. Click **Activate Changes**.
17. Restart the Managed Server for the changes to take affect.

20.1.2.2 Validating the System

You should verify URLs to ensure that the appropriate routing and failover are working.

To verify the URLs:

1. Log in to the CommonDomain Oracle WebLogic Server Administration Console and stop the `HomePageServer_1`, `HomePageServer_2`, and `HomePageServer_3` Managed Servers on `FINHOST1`, `FINHOST2`, and `FINHOST3`.
2. Perform Step 2 in [Section 9.6, "Oracle HTTP Server Configuration,"](#) for the scaled-up server.
3. Access the following URL to verify that routing and failover are functioning properly. (Ensure the log in prompt is visible.)
`https://commonexternal.mycompany.com/homePage/faces/AtkHomePageWelcome`
4. Log in to the CommonDomain Oracle WebLogic Server Administration Console and stop the `HomePageServer_4` Managed Server on `FINHOST3`.
5. Start the `HomePageServer_1` Managed Server on `FINHOST1`.
6. Repeat Step 3. (Ensure the log in prompt is visible.)
7. Start all the Managed Servers on `FINHOST3` and verify that they are running on `FINHOST1` and `FINHOST3`.

20.1.3 Scaling Out the Topology (Adding Managed Servers to a New Node) for Oracle SOA Suite Server

When scaling out the topology, you add new Managed Servers configured to new nodes.

20.1.3.1 Prerequisites for Scaling Out the Topology for Oracle SOA Suite Server

Before you begin, ensure the following:

- Node Manager has been started in the Secure Sockets Layer (SSL) mode by following the instructions in [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"](#)
- You are starting with a clean machine if it is the first time it is being used for a scale out
- The `/etc/hosts` file has proper entries. To verify, ping this machine with the fully qualified name of the machine
- The user created on `FINHOST3` should be the same as the user on `FINHOST1`
- The directory structure `/u01/oracle` is mounted to same shared file system as `FINHOST1`
- The directory structure `/u02/local/oracle/config` on `FINHOST3` has been created
- The initial Oracle Fusion Financials deployment on `FINHOST1` has already been done and verified by provisioning

20.1.3.2 Adding a New Machine in the Oracle WebLogic Server Console

If you have not already added `FINHOST3`, follow these steps:

1. Log in to the Administration Server:
`http://fininternal.mycompany.com:7777/console.`
2. Navigate to **FinancialDomain > Environment > Machines.**
LocalMachine is located in the right-hand pane.
3. In the left-hand pane, click **Lock & Edit.**
4. In the right-hand pane, first click **New** to add the remote machine, and then specify the following:
 - Name - enter `FINHOST3`
 - Machine operating system - Unix
5. Click **Next.**
6. In the window that opens, set the following attributes:
 - Type - SSL
 - Listen Address - `<FINHOST3>`

Note: The "localhost" default value here is wrong.

- Listen port - 5556
7. Click **Finish** and activate the changes.

Note: If you get an error when activating the changes, see [Section 20.8.18, "Administration Console Redirects from Internal URL to Container URL after Activation"](#) for the temporary solution.

20.1.3.3 Packing and Unpacking the Managed Server Domain Home

Since the *FINHOST1* domain directory file system is also available from *FINHOST3*, both the pack and unpack commands can be executed from the *FINHOST3*.

To pack and unpack the Managed Server domain home:

1. Change directory to *ORACLE_BASE*/products/fusionapps/oracle_common/common/bin.

2. Run the pack command. For example, for FinancialDomain:

```
FINHOST3> ./pack.sh -managed=true -domain=ORACLE_BASE/config/domains/  
FINHOST1/FinancialDomain -template=ORACLE_BASE/user_templates/  
FinancialDomain_managed.jar -template_name="Financial_Managed_Server_Domain"
```

3. Run the unpack command:

```
FINHOST3> ./unpack.sh -domain=/u02/local/oracle/config/domains/  
FINHOST3/FinancialDomain -template=ORACLE_BASE/user_templates/FinancialDomain_  
managed.jar
```

Here, *ORACLE_BASE* is shared, and /u02/local is local to *FINHOST3*.

20.1.3.4 Cloning Managed Servers and Assigning Them to FINHOST3

To add a Managed Server and assign it to *FINHOST3*:

1. Log in to the Administration Server:
`http://fininternal.mycompany.com:7777/console.`
2. Navigate to **FinancialDomain > Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the *Managed_Server* checkbox (for example, *soa_server1*) and then click **Clone**.
5. Specify the following Server Identity attributes:
 - Server Name - *soa_server3*

Note: To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to "_3".

- Server Listen Address - *<FINHOST3>*
- Server Listen Port - leave "as is"

Note: For Oracle SOA Suite server, add a port value that is different than the *soa_server1* server value. This will help in server migration.

6. Click **OK**.
7. Navigate back to **FinancialDomain > Environment > Servers**. You now should see the newly cloned sales server, *soa_server3*.
8. Click *soa_server3* and change the following attributes:

- Machine - <FINHOST3>
- Cluster Name - accept the default, SOACluster

Note: Ensure that this cluster name is the same as the cluster name of the original Managed Server.

9. From **soa_server3**, click **Advanced** and then select the **WebLogic Plug-In Enabled** checkbox.
10. Run the newly created Managed Server:
 - a. Navigate to **FinancialDomain > Environment**.
 - b. From the **Navigation** pane on the Oracle WebLogic Server console, select **Activate Changes**.
 - c. Navigate to **FinancialDomain > Environment > Servers > Control**.
 - d. Check the newly created Managed Server and click **Start**.
 - e. Navigate to **FinancialDomain > Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.
11. From the **Name** column, select the scaled-out server, **soa_server3**.
12. Click **Lock & Edit**, and then select the **Configuration** tab.
13. Select the **Keystores** tab, and then ensure that the keystores value is **Custom Identity and Custom Trust**.
14. Do the following:
 - a. Change the Custom Identity Keystore path to point to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/FINHOST3_fusion_identity.jks` file.
 - b. Leave the Custom Identity Keystore type blank.
 - c. Change the Custom Identity Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
 - d. Re-enter the Confirm Custom Identity Keystore Passphrase.
 - e. Ensure that the Confirm Custom Trust Keystore path is pointing to the `ORACLE_BASE/products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks` file.
 - f. Leave the Custom Trust Keystore type blank.
 - g. Change the Custom Trust Keystore Passphrase entry. This should be the same as the `keystorepassword` field described in the first bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
 - h. Re-enter the Custom Trust Keystore Passphrase.
 - i. Click **Save**.
15. Select the **SSL** tab.
 - a. Make sure that Identity and Trust Locations is set to **Keystores**.
 - b. Change the Private Key Alias to `FINHOST3_fusion`.

- c. Change the Private Key Passphrase to the *keypassword*, as described in the second bullet in Step 4 in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#)
- d. Re-enter the *keypassword* from Step c for the Confirm Private Key Passphrase.
- e. Click **Save**.

16. Select the **Server Start tab.**

Change the Arguments to reflect the name of your cloned Managed Server and make sure the server group is the correct cluster name. For example, you should see the following:

```
-DJDBCProgramName\=DS/FinancialDomain/soa_server3  
-Dserver.group\=SOACluster
```

Click **Save**.

17. Select the **Logging tab, and then select the **HTTP** tab.**

18. Do the following:

- a. Change the Log file name to `logs/access.log.%yyyyMMdd%`.
- b. Change the rotation type to **By Time**.
- c. Leave the **Limit number of retained files** option unchecked.
- d. Leave the **Rotate log file on startup** option unchecked.
- e. Click **Save**.
- f. Expand **Advanced**.
- g. Change the format to **Extended**.
- h. Change the extended logging format fields to the following:

```
date time time-taken cs-method cs-uri  
sc-status sc(X-ORACLE-DMS-ECID)  
cs(ECID-Context) cs(Proxy-Remote-User)  
cs(Proxy-Client-IP)
```

- i. Click **Save**.

19. Click **Activate Changes.**

20. Set the following variable:

```
WLST_PROPERTIES="-Dweblogic.security.SSL.trustedCAKeyStore=ORACLE_BASE/  
products/fusionapps/wlserver_10.3/server/lib/fusion_trust.jks"
```

21. Restart the domain's Administration Server on *FINHOST3*:

```
FINHOST3> ORACLE_BASE/products/fusionapps/wlserver_10.3/common/bin/wlst.sh  
  
FINHOST3> nmConnect(username='username', password='password',  
domainName='FinancialDomain', host='FINHOST1',port='5556',  
nmType='ssl', domainDir='/u01/oracle/config/domains/FINHOST1/FinancialDomain')  
  
FINHOST3> nmStart('AdminServer')
```

Note: The *username* and *password* used in the `nmConnect` are the Node Manager credentials (username and password) specified when creating the provisioning response file. This is shown in [Figure 5–3](#) in "Using the Provisioning Process to Install Components for an Enterprise Deployment".

20.1.3.5 Validating the System

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

To verify the URLs:

1. Log in to the FinancialDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on the *FINHOST1* while the Managed Servers on *FINHOST3* are running.
2. Access the following URLs to verify that routing and failover are functioning properly. (Ensure the log in prompt is visible.)
 - `http://fininternal.mycompany.com:7777/soa-infra`
3. Log in to the FinancialDomain Oracle WebLogic Server Administration Console and stop all the Managed Servers on *FINHOST3*.
4. Start the Managed Servers on *FINHOST1*.
5. Repeat Step 2. (Ensure the log in prompt is visible.)
6. Start all the Managed Servers on *FINHOST3* and verify that they are running on *FINHOST1* and *FINHOST3*.

20.1.3.6 Additional Configuration Procedures for Scaling Out Oracle SOA Suite Server

At this point, `soa_server1` and `soa_server3` are running on *FINHOST1* and *FINHOST3*.

Note: For Oracle Fusion Customer Relationship Management, the Oracle SOA Suite virtual IPs for *FINHOST1* and *FINHOST3* are called *FINSOAVH1* and *FINSOAVH3*.

This section includes the following topics:

- [Enabling Virtual IPs on FINHOST3](#)
- [Setting the Listen Address for soa_server3](#)
- [Configuring JMS for the Oracle SOA Suite Server](#)
- [Configuring Oracle Coherence for Deploying Composites](#)
- [Disabling Host Name Verification for the soa_servern Managed Servers](#)
- [Restarting Node Manager on FINHOST3](#)
- [Starting and Validating soa_server3 on FINHOST3](#)

20.1.3.6.1 Enabling Virtual IPs on FINHOST3 To enable the virtual IPs on Linux:

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

1. Run the `ifconfig` command as root:

```
/sbin/ifconfig interface:index IPAddress netmask netmask
```

For example:

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

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

```
/sbin/arping -q -U -c 3 -I interface IPAddress
```

For example:

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

3. Validate that the address is available by pinging it from another node.

For example:

```
/bin/ping 100.200.140.206
```

20.1.3.6.2 Setting the Listen Address for `soa_server3` Ensure that you have performed the steps described in [Section 16.1](#) before setting the `soa_server3` listen address.

To set the listen address for the Managed Server:

1. Log in to the Administration Console.
2. In the Change Center, click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**. The Summary of Servers page is displayed.
5. Select `soa_server3` in the table. The Settings page for `soa_server3` is displayed.
6. Set the **Listen Address** to `FINSOAVH3`.
7. Click **Save**.
8. Click **Activate Changes**.
9. The changes will not take effect until the `soa_server3` Managed Server is restarted (ensure that Node Manager is up and running):
 - a. On the Summary of Servers page, select the **Control** tab.
 - b. Select `soa_server3` in the table and then click **Shutdown**.
 - c. After the server has shut down, select `soa_server3` in the table and then click **Start**.

20.1.3.6.3 Updating the `FusionVirtualHost_fin.conf` Configuration File For information, see [Section 16.4, "Updating the `FusionVirtualHost\_fin.conf` Configuration File."](#)

20.1.3.6.4 Configuring JMS for the Oracle SOA Suite Server After `FINHOST1` has been provisioned, the JMS server and file store are set up and configured for `FINHOST1`. You now must configure the file store for `FINHOST3`. Configure the location for all persistence stores to a directory visible from both nodes.

To configure the file store for *FINHOST3*:

1. Log in to the Oracle WebLogic ServerAdministration Console.
2. In the Domain Structure window, expand the **Services** node and then click the **Persistence Stores** node.
The Summary of Persistence Stores page appears.
3. Click **Lock & Edit**.
4. Click **New**, and then **Create File Store**.
5. Enter a name (for example, *SOAJMSFileStore_auto_3*), and a target, *soa_server3*:
`ORACLE_BASE/config/domains/FINHOST1/FinancialDomain`
6. Click **OK** and activate the changes.
7. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Servers** node.
The Summary of JMS Servers page appears.
8. Click **Lock & Edit**.
9. Click **New**.
10. Enter a name (for example, *SOAJMSServer_3*), then select **SOAJMSFileStore_auto_3** in the Persistence Store dropdown list.
11. Click **Next**.
12. Select *soa_server3* as the target.
13. Click **Finish** and **Activate Changes**.
14. In the Domain Structure window, expand the **Services** node and then click the **Messaging > JMS Modules** node.
The JMS Modules page appears.
15. In the Change Center, click **Lock & Edit**.
16. Click **SOAJMSModule** and then click the **Subdeployments** tab.
17. Select **SOAJMSServer** under **Subdeployments**.
18. Add the new *SOAJMSServer_3* as additional targets for the subdeployment.
19. Click **Save** and **Activate Changes**.

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

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

Multicast communication enables Oracle Fusion Middleware SOA to discover all of the members of a cluster to which it deploys composites dynamically. However,

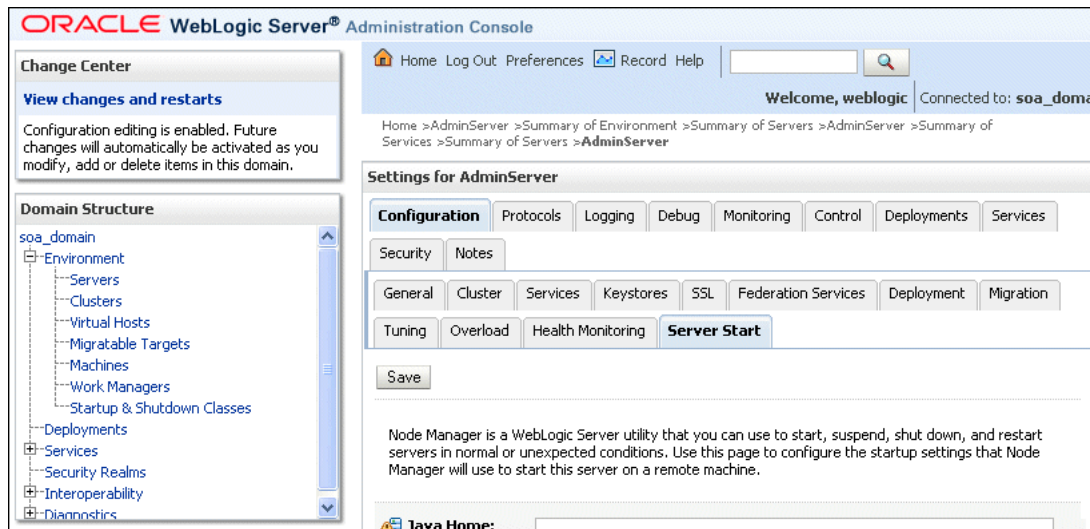
unicast communication does not enable nodes to discover other cluster members in this way. Consequently, you must specify the nodes that belong to the cluster. You do not need to specify all of the nodes of a cluster, however. You need only specify enough nodes so that a new node added to the cluster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

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

Specify the nodes using the `tangosol.coherence.wka.n` system property, where *n* is the number for each Oracle HTTP Server. The numbering starts at 1. This numbering must be sequential and must not contain gaps. In addition, specify the host name used by Oracle Coherence to create a cluster through the `tangosol.coherence.localhost` system property. This local host name should be the virtual host name used by the SOA server as the listener addresses. Set this property by adding the `-Dtangosol.coherence.localhost` parameters to the Arguments field of the Oracle WebLogic Server Administration Console's Server Start tab, shown in [Figure 20–1](#).

Note: *FINSOAVH1* is the virtual host name that maps to the virtual IP where *soa_server1* is listening (in *FINHOST1*). *FINSOAVH3* is the virtual host name that maps to the virtual IP where *soa_server3* is listening (in *FINHOST3*).

Figure 20–1 Setting the Host Name



To add the host name used by Oracle Coherence:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In the Domain Structure window, expand the **Environment** node.
3. Click **Servers**.

The Summary of Servers page appears.

4. Select **soa_server1** (represented as a hyperlink) in the table.
The Settings page appears.
5. Click **Lock & Edit**.
6. Click the **Server Start** tab (shown in [Figure 20-1](#)).
7. Enter the following for soa_server1 and soa_server3 into the **Arguments** field.

For soa_server1, enter the following:

```
-Dtangosol.coherence.wka1=FINSOAVH1
-Dtangosol.coherence.wka2=FINSOAVH3
-Dtangosol.coherence.localhost=FINSOAVH1
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
```

For soa_server3, enter the following:

```
-Dtangosol.coherence.wka1=FINSOAVH3
-Dtangosol.coherence.wka2=FINSOAVH1
-Dtangosol.coherence.localhost=FINSOAVH3
-Dtangosol.coherence.localport=8089
-Dtangosol.coherence.wka1.port=8089
-Dtangosol.coherence.wka2.port=8089
```

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

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

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

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

Note: The Oracle Coherence cluster used for deployment uses port 8088 by default. This port can be changed by specifying the -Dtangosol.coherence.wkaX.port startup parameter.

20.1.3.6.6 Disabling Host Name Verification for the soa_server3 Managed Servers This step is required if you have not set up the appropriate certificates to authenticate the different nodes with the Administration Server. By default, Host Name Verification should be set to None. If it is not, follow the steps below.

If you have not configured the server certificates, you will receive errors when managing the different WebLogic servers. To avoid these errors, disable host name verification while setting up and validating the topology, and enable it again once the enterprise deployment topology configuration is complete.

To disable Host Name Verification:

1. Log in to Oracle WebLogic Server Administration Console. For example, <http://fininternal.mycompany.com:777/console>.
2. Click **Lock & Edit**.
3. Expand the **Environment** node in the Domain Structure window.
4. Click **Servers**.
The Summary of Servers page appears.
5. Select **soa_server3** (represented as a hyperlink) in the table.
The Settings page appears.
6. Select the **SSL** tab.
7. Expand the **Advanced** section of the page.
8. Set **Hostname Verification** to **None**.
9. Click **Save** and activate the changes.

20.1.3.6.7 Restarting Node Manager on FINHOST3 To restart Node Manager on *FINHOST3*, follow the steps in [Section 16.9, "Restarting Node Manager on FINHOST1."](#)

20.1.3.6.8 Starting and Validating soa_server3 on FINHOST3 To start the *soa_server3* Managed Server on *FINHOST3* and ensure that it is configured correctly:

1. From the Administration Console, start the *soa_server3* Managed Server.
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.
3. Access <http://FINSOAVH3:9024/soa-infra> and <http://fininternal.mycompany.com:7777/soa-infra>.

20.1.4 Scaling Up the Topology (Adding Managed Servers to an Existing Node) for Oracle SOA Suite Server

Before performing the procedures in this section, ensure that *CommonDomain* and its Managed Servers are running.

20.1.4.1 Cloning Managed Servers and Assigning Them to FINHOST3

To add a Managed Server and assign it to *FINHOST3*:

1. Log in to the Administration Server:
<http://fininternal.mycompany.com:7777/console>.

2. Navigate to **FinancialDomain > Environment > Servers**.
3. Switch to **Lock & Edit** mode.
4. Select the *Managed_Servers* checkbox (for example, *soa_server3*) and then click **Clone**.
5. Specify the following Server Identity attributes:
 - Server Name - *soa_server4*

Note: To ensure consistency in naming, copy the name of the server shown in **Server Identity** and paste it into the **Server Name** field. Then change the number to "_4".

 - Server Listen Address - *<FINHOST3>*
 - Server Listen Port - leave "Give an unused port on the machine *FINHOST3*"
6. Click **OK**.
7. Navigate back to **FinancialDomain > Environment > Servers**. You now should see the newly cloned SOA server, *soa_server4*.
8. Click *soa_server4* and change the following attributes:
 - Machine - *<FINHOST3>*
 - Cluster Name - Default, *FIN_SOACluster*
9. From *soa_server4*, click **Advanced** and then select the **WebLogic Plug-In Enabled** checkbox.
10. Click **Save**.
11. Run the newly created Managed Servers:
 - a. Navigate to **FinancialDomain > Environment**.
 - b. From the **Navigation** pane on the Oracle WebLogic Server console, select **Activate Changes**.
 - c. Navigate to **FinancialDomain > Environment > Servers > Control**.
 - d. Check the newly created Managed Servers and click **Start**.
 - e. Navigate to **FinancialDomain > Environment > Servers** and check the **State** to verify that the newly created Managed Servers are running.
12. Log in to the Administration Server once again (<http://fininternal.mycompany.com:7777/console>) and verify that all the Managed Servers, including scaled-up servers, are running.

20.1.4.2 Validating the System

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

To verify the URLs:

1. Log in to the FinancialDomain Oracle WebLogic Server Administration Console and stop the *soa_server1*, *soa_server2*, and *soa_server3* Managed Servers on *FINHOST1*, *FINHOST2*, and *FINHOST3*.

2. Perform Step 2 in [Section 9.6, "Oracle HTTP Server Configuration,"](#) for the scaled-up server.
3. Access the following URLs to verify that routing and failover are functioning properly. (Ensure the log in prompt is visible.)
 - `http://fininternal.mycompany.com:7777/soa-infra`
4. Log in to the FinancialDomain Oracle WebLogic Server Administration Console and stop the `soa_server4` Managed Server on `FINHOST3`.
5. Start the Managed Servers on `FINHOST1`.
6. Repeat Step 2. (Ensure the log in prompt is visible.)
7. Start all the Managed Servers on `FINHOST2` and verify that they are running on `FINHOST1`.

20.1.5 Scaling Out the Topology (Adding Managed Servers to a New Node) for Oracle Business Intelligence

When scaling out the topology, you add a new Managed Server and set of system components to a new node in your topology (`FINHOST3`). This procedure assumes that you already have an enterprise topology that includes two nodes, with a Managed Server and a full set of system components on each node.

20.1.5.1 Prerequisites for Scaling Out the Topology for Oracle Business Intelligence

Before performing the steps in this section, ensure that you meet these requirements:

- There must be existing nodes running Oracle Business Intelligence Managed Servers within the topology.
- The new node (`FINHOST3`) can access the existing home directories for Oracle WebLogic Server and Oracle Business Intelligence.
- When an `FA_MW_HOME` or `WL_HOME` is shared by multiple servers in different nodes, it is recommended that you keep the Oracle Inventory and Middleware home list in those nodes updated for consistency in the installations and application of patches. To update the `oraInventory` in a node and "attach" an installation in a shared storage to it, use `ORACLE_BASE/products/fusionapps/bi/oui/bin/attachHome.sh`. To update the Middleware home list to add or remove a `WL_HOME`, edit the `ORACLE_BASE/products/fusionapps/.home` file. See the steps below.
- You must ensure that all shared storage directories are available on the new node. Ensure that all shared directories are available on all nodes, except for the `ORACLE_INSTANCE` directory and the domain directory for the scaled-out Managed Server.

Also, if you are using shared storage for the identity keystore and trust keystore that hold your host name verification certificates, make sure that the shared storage directory is accessible from the scaled-out node (`FINHOST3`). If you are using local directories for your keystores, follow the steps in [Section 7.2, "Creating the Identity Keystore on FINHOST2."](#) to create and configure a local identity keystore for the scaled-out node.

For example, mount the following directories:

- Transaction Log directory
- JMS Persistence Store

- Global Cache
- BI Presentation Catalog
- BI Repository Publishing directory
- BI Publisher Catalog
- BI Publisher Configuration Keystore (certs)
- *MW_HOME*

20.1.5.2 Scale-Out Procedure for Oracle Business Intelligence

To scale out Oracle Business Intelligence on *FINHOST3*:

1. On *FINHOST3*, mount the existing Middleware home, which should include the Oracle Business Intelligence installation and (optionally, if the domain directory for Managed Servers in other nodes resides on shared storage) the domain directory, and ensure that the new node has access to this directory, just like the rest of the nodes in the domain.
2. Run the following command to attach *ORACLE_BASE/products/fusionapps/oracle_common* in shared storage to the local Oracle Inventory:

```
FINHOST3> cd ORACLE_BASE/products/fusionapps/oracle_common/oui/bin/
FINHOST3> ./attachHome.sh -jreLoc ORACLE_BASE/products/fusionapps/jdk6
```

To update the Middleware home list, create (or edit, if another WebLogic installation exists in the node) the *ORACLE_BASE/products/fusionapps/.home* file and add *ORACLE_BASE/products/fusionapps* to it.

3. Start Node Manager:
 - a. Stop any Node Manager running on *FINHOST3*.
 - b. Change directory to *ORACLE_BASE/products/fusionapps/wlserver_10.3/common/nodemanager* and edit the *nodemanager.properties* file with the following:


```
SecureListener=false
```
 - c. Change directory to *ORACLE_BASE/products/fusionapps/oracle_common/common/bin* and run the following script:


```
./setNMProps.sh
```
 - d. Change directory to *ORACLE_BASE/products/fusionapps/wlserver_10.3/server/bin* and run the following script:


```
./startNodeManager.sh
```

Node Manager starts on *FINHOST3*.

Note: Steps b through d will enable Node Manager on *FINHOST3* and the Administrator Console to communicate on Plain Socket.

4. Run the Configuration Assistant from one of the shared Oracle homes, using the steps in [Section 15.5.1, "Scaling Out the Oracle Business Intelligence System on FINHOST2"](#) as a guide.

5. Scale out the system components on *FINHOST3*, using the steps in [Section 15.5.3, "Scaling Out the System Components"](#) as a guide.
6. Configure the *bi_server3* Managed Server by setting the Listen Address and disabling host name verification, using the steps in [Section 15.5.5, "Configuring the *bi_server2* Managed Server"](#) as a guide.
7. Configure JMS for Oracle BI Publisher, as described in [Section 15.5.6.3.3, "Configuring JMS for BI Publisher."](#)
8. Configure Oracle BI for Microsoft Office on *FINHOST3*, as described in [Section 15.5.6.4, "Additional Configuration Tasks for Oracle BI for Microsoft Office."](#)
9. Set the location of the default persistence store for *bi_server3*, as described in [Section 15.5.7, "Configuring a Default Persistence Store for Transaction Recovery."](#)
10. Configure Oracle HTTP Server for *BIVH3* using the steps in [Section 15.4.3, "Updating the *FusionVirtualHost_bi.conf* Configuration File"](#) as a guide.
11. Start the *bi_server3* Managed Server and the system components running on *FINHOST3*. See [Section 15.5.8, "Starting and Validating Oracle Business Intelligence on *FINHOST2*"](#) for details.
12. Set up server migration for the new node, as described in the following sections:
 - [Section 7.2, "Creating the Identity Keystore on *FINHOST2*"](#)
 - [Section 18.2.4, "Editing Node Manager's Properties File"](#)
 - [Section 18.2.5, "Setting Environment and Superuser Privileges for the *wlsifconfig.sh* Script"](#)
 - [Section 18.2.6, "Configuring Server Migration Targets"](#)
 - [Section 18.2.7, "Testing the Server Migration"](#)
13. Access the following URLs to validate the configuration:
 - <http://BIVH3:10217/analytics> to verify the status of *bi_server3*.
 - <http://BIVH3:10217/wsm-pm> to verify the status of Web Services Manager. Click **Validate Policy Manager**. A list of policies and assertion templates available in the data is displayed.

Note: The configuration is incorrect if no policies or assertion templates appear.

- <http://BIVH3:10217/xmlpserver> to verify the status of the Oracle BI Publisher application.
- <http://BIVH3:10217/ui> to verify the status of the Oracle Real-Time Decisions application.
- <http://BIVH3:10217/mapviewer> to verify the status of the map view functionality in Oracle BI EE.
- <http://BIVH3:10217/hr> to verify Financial Reporting.
- <http://BIVH3:10217/calcmgr/index.htm> to verify Calculation Manager.
- <http://BIVH3:10217/aps/Test> to verify APS.
- <http://BIVH3:10217/workspace> to verify workspace

Oracle recommends using host name verification for the communication between Node Manager and the servers in the domain. This requires the use of certificates for the different addresses communicating with the Administration Server and other servers. See [Chapter 7, "Setting Up Node Manager for an Enterprise Deployment"](#) for further details.

20.1.6 Scaling Up the Topology for Oracle Business Intelligence

This procedure assumes that you already have an enterprise topology that includes two nodes, with a Managed Server and a full set of system components on each node. To scale up the topology, you increase the number of system components running on one of your existing nodes.

Note that it is not necessary to run multiple Managed Servers on a given node.

20.1.6.1 Scale-Up Procedure for Oracle Business Intelligence

To scale up Oracle Business Intelligence on *FINHOST3*:

1. Log in to Fusion Middleware Control.
2. Expand the **Business Intelligence** node in the Farm_BIDomain window.
3. Click **coreapplication**.
4. Click **Capacity Management**, then click **Scalability**.
5. Click **Lock & Edit** and then change the number of BI Servers, Presentation Servers, or JavaHosts using the arrow keys.

Note: To avoid port conflicts for the system components being scaled within the given Oracle WebLogic Server instance, enter a different range of available ports in the **Port Range From** and **Port Range To** fields. For example, change **Port Range From** to 10221 and **Port Range To** to 10300.

6. Click **Apply**, then click **Activate Changes**.
7. Click **Restart** to apply recent changes.
8. Click **Restart** under **Manage System**.
9. Click **Yes** in the confirmation dialog.

20.2 Performing Backups and Recoveries

[Table 20–1](#) lists the static artifacts to back up in the 11g Oracle Fusion Financials enterprise deployment.

Table 20–1 Static Artifacts to Back Up in the 11g CRM Enterprise Deployment

| Type | Host | Location | Tier |
|------------------------------|---|--|-----------|
| ORACLE HOME (DB) | <i>FUSIONDBHOST1</i>
and
<i>FUSIONDBHOST2</i> | The location is user-defined. Generally, /u01/oracle. | Data tier |
| MW HOME (Oracle HTTP Server) | <i>WEBHOST1</i> and
<i>WEBHOST2</i> | <i>ORACLE_BASE</i> /products
<i>ORACLE_BASE</i> /config | Web tier |

Table 20–1 (Cont.) Static Artifacts to Back Up in the 11g CRM Enterprise Deployment

| Type | Host | Location | Tier |
|----------------------------|--------------------------|--|------------------|
| MW HOME (/APPS_HOME) | FINHOST1 and
FINHOST2 | ORACLE_BASE/products
ORACLE_BASE/config | Application tier |
| Installation-related files | | /u01/oracle/repository,
OraInventory, .home, oraInst.loc,
oratab | N/A |

Table 20–2 lists the run-time artifacts to back up in the 11g Oracle Fusion Financials enterprise deployment.

Table 20–2 Run-Time Artifacts to Back Up in the 11g CRM Enterprise Deployment

| Type | Host | Location | Tier |
|---|------------------------------------|--|------------------|
| DOMAIN HOME | FINHOST1 and
FINHOST2 | /u02/local/oracle/config/domains/HOSTNAME/domain_name | Application tier |
| Application artifacts (EAR and WAR files) | FINHOST1 and
FINHOST2 | Find the application artifacts by viewing all of the deployments through the administration console. | Application tier |
| Oracle HTTP Server instance home | WEBHOST1 and
WEBHOST2 | ORACLE_BASE/config/CommonDomain_webtier | Web tier |
| Oracle RAC databases | FUSIONDBHOST1 and
FUSIONDBHOST2 | The location is user-defined. | Data tier |

For more information on backup and recovery of Oracle Fusion Middleware components, see *Oracle Fusion Middleware Administrator's Guide*.

20.3 Monitoring the Topology

For information on monitoring the Oracle Fusion Customer Relationship Management topology, see the following documents:

- *Oracle Fusion Middleware System Administrator's Guide for Content Server*
- *Oracle Fusion Middleware Application Administrator's Guide for Content Server*
- *Oracle Fusion Middleware Administrator's Guide for Imaging and Process Management*

20.4 Migrating from a Test Environment to a Production Environment

For information, see "Moving Components for Oracle Fusion Applications Across Environments" in the *Oracle Fusion Applications Administrator's Guide*.

20.5 Configuring Log File Rotation

An ODL log is a set of log files that includes the current ODL log file and zero or more ODL Archives (segment files) that contain older messages. As the log file grows, new information is added to the end of the log file, *server_name-diagnostic.log*. When the log file reaches the rotation point, it is renamed and a new log file, *server_name-diagnostic.log* is created. You specify the rotation point, by specifying the maximum ODL segment size, or, for the log files of some components, the rotation time and rotation frequency.

Segment files are created when the ODL log file *server_name*-diagnostic.log reaches the rotation point. That is, the *server_name*-diagnostic.log is renamed to *server_name*-diagnostic-*n*.log, where *n* is an integer, and a new *server_name*-diagnostic.log file is created when the component generates new diagnostic messages.

To limit the size of the ODL log, you can specify:

- The maximum size of the logging directory. Whenever the sum of the sizes of all of the files in the directory reaches the maximum, the oldest archive is deleted to keep the total size under the specified limit.

By default, the log files are rotated when they reach 10 MB. The maximum size of all log files for a particular component is 100 MB.

- The maximum size of the log file. You specify that a new log file be created when a specific time or frequency is reached.

Note: After you change the log file rotation, the configuration is reloaded dynamically. It may take 1 or 2 seconds to reload the configuration.

The following topics describe how to change the rotation:

- [Section 20.5.1, "Specifying Log File Rotation Using Oracle Enterprise Manager"](#)
- [Section 20.5.2, "Specifying Log File Rotation Using WLST"](#)

20.5.1 Specifying Log File Rotation Using Oracle Enterprise Manager

To configure log file rotation using Oracle Enterprise Manager for a component:

1. Log in to the component (for example, <http://crminternal.mycompany.com/em>).
2. From the navigation pane, select the component (for example, navigate to **Farm_CommonDomain > WebLogic Domain > CommonDomain > ESSCluster > ess_server1**).
3. Select **ess_server1**.
4. From the WebLogic Server dropdown list, select **Logs > Log Configuration**, then select the **Log Files** tab.

Note: The WebLogic Server dropdown list is located at the top left corner of the right panel.

5. In the table, select the logger and click **Edit Configuration**.

The Edit Log File dialog box is displayed.

6. In the Rotation Policy section, you can select one of the following:

- **Size Based:** If you select this, enter the following:
 - For **Maximum Log File Size**, enter the size in MB, for example, 15.
 - For **Maximum Size of All Log Files**, enter the size in MB, for example, 150.
- **Time Based:** If you select this, enter the following:

- For **Start Time**, enter the date when you want the rotation to start. For example, enter 10-SEP-2009.
- For **Frequency**, you can select **Minutes** and enter the number of minutes, or you can select **Hourly**, **Daily**, or **Weekly**.
- For **Retention Period**, you can specify how long the log files are kept. You can select **Minutes** and enter the number of minutes, or you can specify **Day**, **Week**, **Month**, or **Year**.

Specifying a shorter period means that you use less disk space, but are not able to retrieve older information.

7. Click **OK**.
8. In the confirmation window, click **Close**.

20.5.2 Specifying Log File Rotation Using WLST

To specify log file rotation using WLST, use the `configureLogHandler` command. You can specify size-based rotation or time-based rotation.

For example, to specify that the log files rotate daily and that they are retained for a week, use the following command:

```
configureLogHandler(name='odl-handler', rotationFrequency='daily',  
                    retentionPeriod='week')
```

To specify that the size of a log file does not exceed 5MB and rotates when it reaches that size, use the following command:

```
configureLogHandler(name='odl-handler', maxFileSize='5M')
```

20.6 Patching the Topology

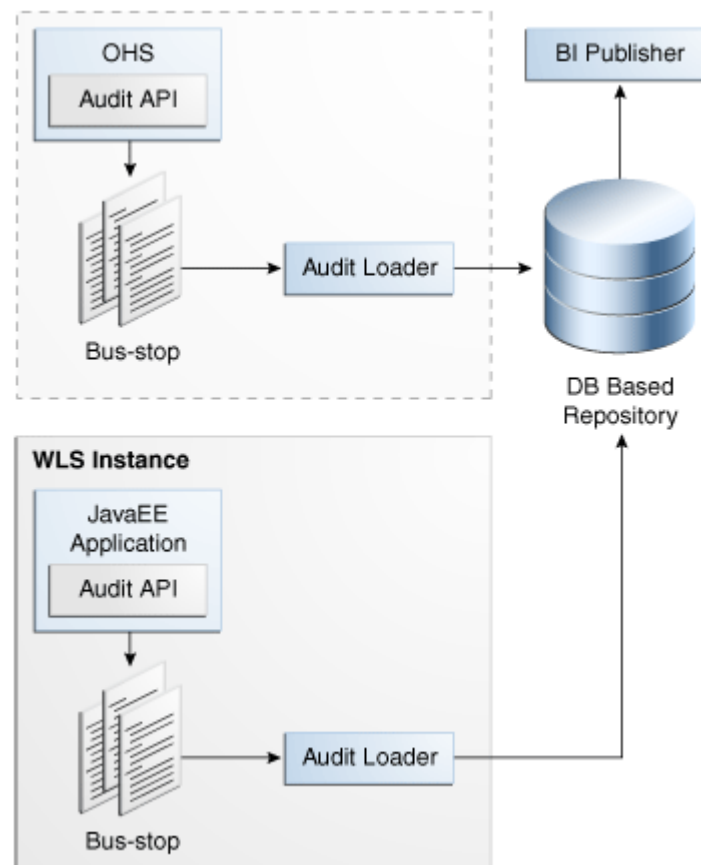
For information, see the *Oracle Fusion Applications Patching Guide*.

20.7 Auditing

Oracle Fusion Middleware Audit Framework is a new service in Oracle Fusion Middleware 11g, designed to provide a centralized audit framework for the middleware family of products. The framework provides audit service for platform components such as Oracle Platform Security Services (OPSS) and Oracle Web Services. It also provides a framework for JavaEE applications, starting with Oracle's own JavaEE components. JavaEE applications will be able to create application-specific audit events. For non-JavaEE Oracle components in the middleware, such as C or JavaSE components, the audit framework also provides an end-to-end structure similar to that for JavaEE applications.

[Figure 20–2](#) is a high-level architectural diagram of the Oracle Fusion Middleware Audit Framework.

Figure 20–2 Audit Event Flow



The Oracle Fusion Middleware Audit Framework consists of the following key components:

- **Audit APIs:** These are APIs provided by the audit framework for any audit-aware components integrating with the Oracle Fusion Middleware Audit Framework. During run time, applications may call these APIs, where appropriate, to audit the necessary information about a particular event happening in the application code. The interface allows applications to specify event details such as user name and other attributes needed to provide the context of the event being audited.
- **Audit Events and Configuration:** The Oracle Fusion Middleware Audit Framework provides a set of generic events for convenient mapping to application audit events. Some of these include common events such as authentication. The framework also allows applications to define application-specific events.

These event definitions and configurations are implemented as part of the audit service in Oracle Platform Security Services. Configurations can be updated through Enterprise Manager (UI) and WebLogic Scripting Tool (WLST) command-line tool.

- **Audit Bus-stop:** Bus-stops are local files containing audit data before they are pushed to the audit repository. In the event where no database repository is configured, these bus-stop files can be used as a file-based audit repository. The bus-stop files are simple text files that can be queried easily to look up specific audit events. When a DB-based repository is in place, the bus-stop acts as an intermediary between the component and the audit repository. The local files are

periodically uploaded to the audit repository based on a configurable time interval.

- **Audit Loader:** As the name implies, the audit loader loads the files from the audit bus-stop into the audit repository. In the case of platform and JavaEE application audit, the audit loader is started as part of the JavaEE container start-up. In the case of system components, the audit loader is a periodically spawned process.
- **Audit Repository:** The audit repository contains a predefined Oracle Fusion Middleware Audit Framework schema, created by Repository Creation Utility (RCU). Once configured, all the audit loaders are aware of the repository and upload data to it periodically. The audit data in the audit repository is expected to be cumulative and will grow over time. Ideally, this should not be an operational database used by any other applications; rather, it should be a standalone RDBMS used for audit purposes only. In a highly available configuration, Oracle recommends that you use an Oracle Real Application Clusters (RAC) database as the audit data store.
- **Oracle Business Intelligence Publisher:** The data in the audit repository is exposed through predefined reports in Oracle Business Intelligence Publisher. The reports allow users to drill down the audit data based on various criteria. For example:
 - User name
 - Time range
 - Application type
 - Execution context identifier (ECID)

For more introductory information for the Oracle Fusion Middleware Audit Framework, see the "Introduction to Oracle Fusion Middleware Audit Framework" chapter in the *Oracle Fusion Middleware Application Security Guide*.

For information on how to configure the repository for Oracle Fusion Middleware Audit Framework, see the "Configuring and Managing Auditing" chapter in the *Oracle Fusion Middleware Application Security Guide*.

The enterprise deployment topology does not include Oracle Fusion Middleware Audit Framework configuration. The ability to generate audit data to the bus-stop files and the configuration of the audit loader will be available once the products are installed. The main consideration is the audit database repository where the audit data is stored. Because of the volume and the historical nature of the audit data, it is strongly recommended that customers use a separate database from the operational store or stores being used for other middleware components.

20.8 Troubleshooting

This section covers the following topics:

- [Section 20.8.1, "Page Not Found When Accessing soa-infra Application Through Load Balancer"](#)
- [Section 20.8.2, "soa-infra Application Fails to Start Due to Deployment Framework Issues \(Coherence\)"](#)
- [Section 20.8.3, "Incomplete Policy Migration After Failed Restart of SOA Server"](#)
- [Section 20.8.4, "Oracle SOA Suite Server Fails to Start Due to Maximum Number of Processes Available in Database"](#)

- [Section 20.8.5, "Administration Server Fails to Start After a Manual Failover"](#)
- [Section 20.8.6, "Error While Activating Changes in Administration Console"](#)
- [Section 20.8.7, "SOA Server Not Failed Over After Server Migration"](#)
- [Section 20.8.8, "SOA Server Not Reachable From Browser After Server Migration"](#)
- [Section 20.8.9, "Oracle Access Manager Configuration Tool Does Not Remove URLs"](#)
- [Section 20.8.10, "Redirecting of Users to Login Screen After Activating Changes in Administration Console"](#)
- [Section 20.8.11, "Redirecting of Users to Administration Console's Home Page After Activating Changes to OAM"](#)
- [Section 20.8.12, "Configured JOC Port Already in Use"](#)
- [Section 20.8.13, "Out-of-Memory Issues on Managed Servers"](#)
- [Section 20.8.14, "JDBC Connection Reset Appears When on OEL 5.4"](#)
- [Section 20.8.15, "Missing JMS Instances on Oracle BI Publisher Scheduler Diagnostics Page"](#)
- [Section 20.8.16, "Oracle BI Publisher Jobs in Inconsistent State After Managed Server Shutdown"](#)
- [Section 20.8.17, "JMS Instance Fails in an Oracle BI Publisher Cluster"](#)
- [Section 20.8.18, "Administration Console Redirects from Internal URL to Container URL after Activation"](#)

20.8.1 Page Not Found When Accessing soa-infra Application Through Load Balancer

Problem: A 404 "page not found" message is displayed in the web browser when you try to access the soa-infra application using the load balancer address. The error is intermittent and Oracle SOA Suite servers appear as "Running" in the WLS Administration Console.

Solution: Even when the Oracle SOA Suite Managed Servers may be up and running, some of the applications contained in them may be in Admin, Prepared or other states different from Active. The soa-infra application may be unavailable while the Oracle SOA Suite server is running. Check the Deployments page in the Administration Console to verify the status of the soa-infra application. It should be in "Active" state. Check the Oracle SOA Suite server's output log for errors pertaining to the soa-infra application and try to start it from the Deployments page in the Administration Console.

20.8.2 soa-infra Application Fails to Start Due to Deployment Framework Issues (Coherence)

Problem: The soa-infra application fails to start after changes to the Coherence configuration for deployment have been applied. The Oracle SOA Suite server output log reports the following:

```
Cluster communication initialization failed. If you are using multicast, Please
make sure multicast is enabled on your network and that there is no interference
on the address in use. Please see the documentation for more details.
```

Solutions:

- When using multicast instead of unicast for cluster deployments of Oracle SOA Suite composites, a message similar to the above may appear if a multicast conflict arises when starting the soa-infra application (that is, starting the Managed Server on which Oracle SOA Suite runs). These messages, which occur when Oracle Coherence throws a run-time exception, also include the details of the exception itself. If such a message appears, check the multicast configuration in your network. Verify that you can ping multicast addresses. In addition, check for other clusters that may have the same multicast address but have a different cluster name in your network, as this may cause a conflict that prevents soa-infra from starting. If multicast is not enabled in your network, you can change the deployment framework to use unicast as described in *Oracle Coherence Developer's Guide*.
- When entering well-known address list for unicast (in server start parameters), make sure that the node's addresses entered for the localhost and clustered servers are correct. Error messages like the following are reported in the server's output log if any of the addresses is not resolved correctly:

```
oracle.integration.platform.blocks.deploy.CompositeDeploymentCoordinatorMessage
s errorUnableToStartCoherence
```

20.8.3 Incomplete Policy Migration After Failed Restart of SOA Server

Problem: The SOA server fails to start through the administration console *before* setting Node Manager property `startScriptEnabled=true`. The server does not come up after the property is set either. The SOA Server output log reports the following:

```
SEVERE: <.> Unable to Encrypt data
Unable to Encrypt data.
Check installation/post-installation steps for errors. Check for errors during SOA
server startup.

ORABPEL-35010
.
Unable to Encrypt data.
Unable to Encrypt data.
Check installation/post-installation steps for errors. Check for errors
during SOA server startup.
.
at
oracle.bpel.services.common.util.EncryptionService.encrypt(EncryptionService.java:
56)
...
```

Solution: Incomplete policy migration results from an unsuccessful start of the first SOA server in a cluster. To enable full migration, edit the `<jazn-policy>` element the `system-jazn-data.xml` file to grant permission to `bpm-services.jar`:

```
<grant>
  <grantee>
    <codesource>
<url>file:${oracle.home}/soa/modules/oracle.soa.workflow_11.1.1/bpm-services.jar
</url>
    </codesource>
  </grantee>
  <permissions>
    <permission>
      <class>java.security.AllPermission</class>
    </permission>
```

```
</permissions>
</grant>
```

20.8.4 Oracle SOA Suite Server Fails to Start Due to Maximum Number of Processes Available in Database

Problem: A Oracle SOA Suite server fails to start. The domain has been extended for new types of Managed Server or the system has been scaled up (added new servers of the same type). The Oracle SOA Suite server output log reports the following:

```
<Warning> <JDBC> <BEA-001129> <Received exception while creating connection for
pool "SOADatasource-rac0": Listener refused the connection with the following
error:
```

```
ORA-12516, TNS:listener could not find available handler with matching protocol
stack >
```

Solution: Verify the number of processes in the database and adjust accordingly. As the SYS user, issue the `SHOW PARAMETER` command:

```
SQL> SHOW PARAMETER processes
```

Set the initialization parameter using the following command:

```
SQL> ALTER SYSTEM SET processes=greater than 2500 SCOPE=SPFILE
```

Restart the database.

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

20.8.5 Administration Server Fails to Start After a Manual Failover

Problem: Administration Server fails to start after the Administration Server node failed and manual failover to another nodes is performed. The Administration Server output log reports the following:

```
<Feb 19, 2009 3:43:05 AM PST> <Warning> <EmbeddedLDAP> <BEA-171520> <Could not
obtain an exclusive lock for directory: ORACLE_BASE/admin/edg_domain/aserver/edg_
domain/servers/AdminServer/data/ldap/ldapfiles. Waiting for 10 seconds and then
retrying in case existing WebLogic Server is still shutting down.>
```

Solution: When restoring a node after a node crash and using shared storage for the domain directory, you may see this error in the log for the Administration Server due to unsuccessful lock cleanup. To resolve this error, remove the file `ORACLE_HOME/config/domains/FINHOST1/DomainName/servers/AdminServer/data/ldap/ldapfiles/EmbeddedLDAP.lock`.

20.8.6 Error While Activating Changes in Administration Console

Problem: Activation of changes in Administration Console fails after changes to a server's start configuration have been performed. The Administration Console reports the following when clicking **Activate Changes**:

```
An error occurred during activation of changes, please see the log for details.
```

[Management:141190]The commit phase of the configuration update failed with an exception:

In production mode, it's not allowed to set a clear text value to the property: PasswordEncrypted of ServerStartMBean

Solution: This may happen when start parameters are changed for a server in the Administration Console. In this case, provide user name/password information in the server start configuration in the Administration Console for the specific server whose configuration was being changed.

20.8.7 SOA Server Not Failed Over After Server Migration

Problem: After reaching the maximum restart attempts by local Node Manager, Node Manager in the failover node tries to restart it, but the server does not come up. The server seems to be failed over as reported by Node Manager's output information. The VIP used by the SOA server is not enabled in the failover node after Node Manager tries to migrate it (if config in the failover node does not report the VIP in any interface). Executing the command `sudo ifconfig $INTERFACE $ADDRESS $NETMASK` does not enable the IP in the failover node.

Solution: The rights and configuration for `sudo` execution should not prompt for a password. Verify the configuration of `sudo` with your system administrator so that `sudo` works without a password prompt.

20.8.8 SOA Server Not Reachable From Browser After Server Migration

Problem: Server migration is working (SOA server is restarted in the failed over node), but the `Virtual_Hostname:8001/soa-infra` URL cannot be accessed in the web browser. The server has been "killed" in its original host and Node Manager in the failover node reports that the VIP has been migrated and the server started. The VIP used by the SOA server cannot be pinged from the client's node (that is, the node where the browser is being used).

Solution: The `arping` command executed by Node Manager to update ARP caches did not broadcast the update properly. In this case, the node is not reachable to external nodes. Either update the `nodemanager.properties` file to include the `MACBroadcast` or execute a manual `arping`:

```
/sbin/arping -b -q -c 3 -A -I INTERFACE ADDRESS > $NullDevice 2>&1
```

Where `INTERFACE` is the network interface where the virtual IP is enabled and `ADDRESS` is the virtual IP address.

20.8.9 Oracle Access Manager Configuration Tool Does Not Remove URLs

Problem: The Oracle Access Manager Configuration Tool has been used and a set of URLs was added to the policies in Oracle Access Manager. One of multiple URLs had a typo. Executing the Oracle Access Manager Configuration Tool again with the correct URLs completes successfully; however, when accessing Policy Manager, the incorrect URL is still there.

Solution: The Oracle Access Manager Configuration Tool only adds new URLs to existing policies when executed with the same `app_domain` name. To remove a URL, use the Policy Manager Console in Oracle Access Manager. Log on to the Access Administration site for Oracle Access Manager, click on My Policy Domains, click on

the created policy domain (SOA_EDG), then on the Resources tab, and remove the incorrect URLs.

20.8.10 Redirecting of Users to Login Screen After Activating Changes in Administration Console

Problem: After configuring Oracle HTTP Server and LBR to access the Oracle WebLogic Administration Console, some activation changes cause the redirection to the login screen for the Administration Console.

Solution: This is the result of the console attempting to follow changes to port, channel, and security settings as a user makes these changes. For certain changes, the console may redirect to the Administration Server's listen address. Activation is completed regardless of the redirection. It is not required to log in again; users can simply update the URL to `fin.mycompany.com/console/console.portal` and directly access the home page for the Administration Console.

Note: This problem will not occur if you have disabled tracking of the changes described in this section.

20.8.11 Redirecting of Users to Administration Console's Home Page After Activating Changes to OAM

Problem: After configuring OAM, some activation changes cause the redirection to the Administration Console's home page (instead of the context menu where the activation was performed).

Solution: This is expected when OAM SSO is configured and the Administration Console is set to follow configuration changes (redirections are performed by the Administration Server when activating some changes). Activations should complete regardless of this redirection. For successive changes not to redirect, access the Administration Console, select Preferences, then Shared Preferences, and unselect the "Follow Configuration Changes" check box.

20.8.12 Configured JOC Port Already in Use

Problem: Attempts to start a Managed Server that uses the Java Object Cache (JOC), such as OWSM Managed Servers, fail. The following errors appear in the logs:

```
J2EE JOC-058 distributed cache initialization failure
J2EE JOC-043 base exception:
J2EE JOC-803 unexpected EOF during read.
```

Solution: Another process is using the same port that JOC is attempting to obtain. Either stop that process, or reconfigure JOC for this cluster to use another port in the recommended port range.

20.8.13 Out-of-Memory Issues on Managed Servers

Problem: You are experiencing out-of-memory issues on Managed Servers.

Solution: Increase the size of the memory heap allocated for the Java VM to at least one gigabyte:

1. Log in to the Oracle WebLogic Administration Console.
2. Click **Environment**, then **Servers**.

3. Click on a Managed Server name.
4. Open the **Configuration** tab.
5. Open the **Server Start** tab in the second row of tabs.
6. Include the memory parameters in the **Arguments** box, for example:

```
-Xms3072m -Xmx1024m -XX:CompileThreshold=8000 -XX:PermSize=128m
-XX:MaxPermSize=1024m
```

Note: Please note that the memory parameter requirements may differ between various JVMs (Sun, JRockit, or others). See "Increasing the Java VM Heap Size for Managed Servers" in the *Oracle Fusion Middleware Installation Guide for Oracle Enterprise Content Management Suite* for further details.

7. Save the configuration changes.
8. Restart all running Managed Servers.

20.8.14 JDBC Connection Reset Appears When on OEL 5.4

Problem: When you are on Oracle Enterprise Linux (OEL) 5.4, a Java Database Connectivity (JDBC) connection reset appears.

Solutions:

- Upgrade to OEL 5.6.
- As root, do the following:
 1. Download and install the rngd tool.
 2. Execute the following commands (in order):


```
rngd -r /dev/urandom -o /dev/random
```

```
cat /proc/sys/kernel/random/entropy_avail
```
 3. Ensure that entropy returns a number greater than 1000.

20.8.15 Missing JMS Instances on Oracle BI Publisher Scheduler Diagnostics Page

In some cases, only one JMS instance is visible on the Oracle BI Publisher Scheduler diagnostics page, rather than all instances in the cluster. This issue is most likely caused by clocks being out of sync. For more information on the importance of synchronizing clocks on all nodes in the cluster, see "Clock Synchronization" in the chapter "Database and Environment Preconfiguration" in *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence*.

20.8.16 Oracle BI Publisher Jobs in Inconsistent State After Managed Server Shutdown

Before shutting down the Managed Server on which Oracle BI Publisher is running, it is a best practice (but not mandatory) to wait for all running Oracle BI Publisher jobs to complete, or to cancel any unfinished jobs using the Report Job History page. Otherwise, the shutdown might cause some jobs to incorrectly stay in a running state.

20.8.17 JMS Instance Fails in an Oracle BI Publisher Cluster

On rare occasions, a JMS instance is missing from an Oracle BI Publisher Scheduler cluster. To resolve this issue, restart the Oracle BI Publisher application from the Oracle WebLogic Server Administration Console.

To restart Oracle BI Publisher:

1. Log in to the Administration Console.
2. Click **Deployments** in the Domain Structure window.
3. Select **bipublisher(11.1.1)**.
4. Click **Stop**.
5. After the application stops, click **Start**.

20.8.18 Administration Console Redirects from Internal URL to Container URL after Activation

Log in to the Administration Console and do the following:

1. Click **Preferences** in the top navigation bar.
2. Select the **Shared Preferences** tab.
3. De-select **Follow Configuration Changes**.
4. Click **Save**.

Deploying Administrative Clients for Oracle Fusion Applications

In typical Oracle Fusion Applications deployment there are a number of administrative clients, or thick clients, from which end users (functional administrators) must have direct access to application servers or file systems via Hypertext Transfer Protocol (HTTP) or socket connections.

Some administrative-client applications are the following:

- FR (Financial Reporting) Studio
- Oracle BI Enterprise Edition Administrative client
- Oracle Business Intelligence Catalog Manager
- Oracle Imaging and Process Management document-provider clients, such as
 - Oracle Forms Recognition (OFR Verifier, OFR Designer)
 - Oracle Document Capture
 - Mail Server for Oracle Document Capture
 - Inbound fax tools
- File Transfer Protocol (FTP) Server (and the ability for the end user to upload files)
- Oracle JDeveloper
- ODI (Oracle Data Integrator) Studio

Thick clients are usually installed on Windows servers, which sometimes sit unattended on end users' desktops at a customer location. Such open connections to sensitive data (such as that housed in a data center) are highly vulnerable to security breaches, and security best practices generally do not allow this kind of configuration.

This chapter describes how to address these security loopholes.

A.1 Recommended Solution

In order to close potential security loopholes, all administrative thick clients should be installed on host Windows servers that have secured HTTP remote desktop connections (RDCs). These servers should be located in each data center.

A separate administrative subnet, acting like an administrative demilitarized zone (DMZ) for thick clients, should be created in each data center to host the Windows servers.

End users (customers) will access the thick clients by logging in to the Windows servers through a virtual private network (VPN), and either a secured HTTP RDC or socket connection. Only the thick clients on the Windows servers in the administrative subnet will have access to application servers or file systems in a data center.

Note: Since some client components, such as Oracle Imaging and Process Management and FTP, are only integrated with socket connections, enforcing VPN access is required.

Figure A-1 shows the overall topology of the administrative subnet and its client components. Figure A-2 shows the topology details.

Figure A-1 Administrative Subnet Topology

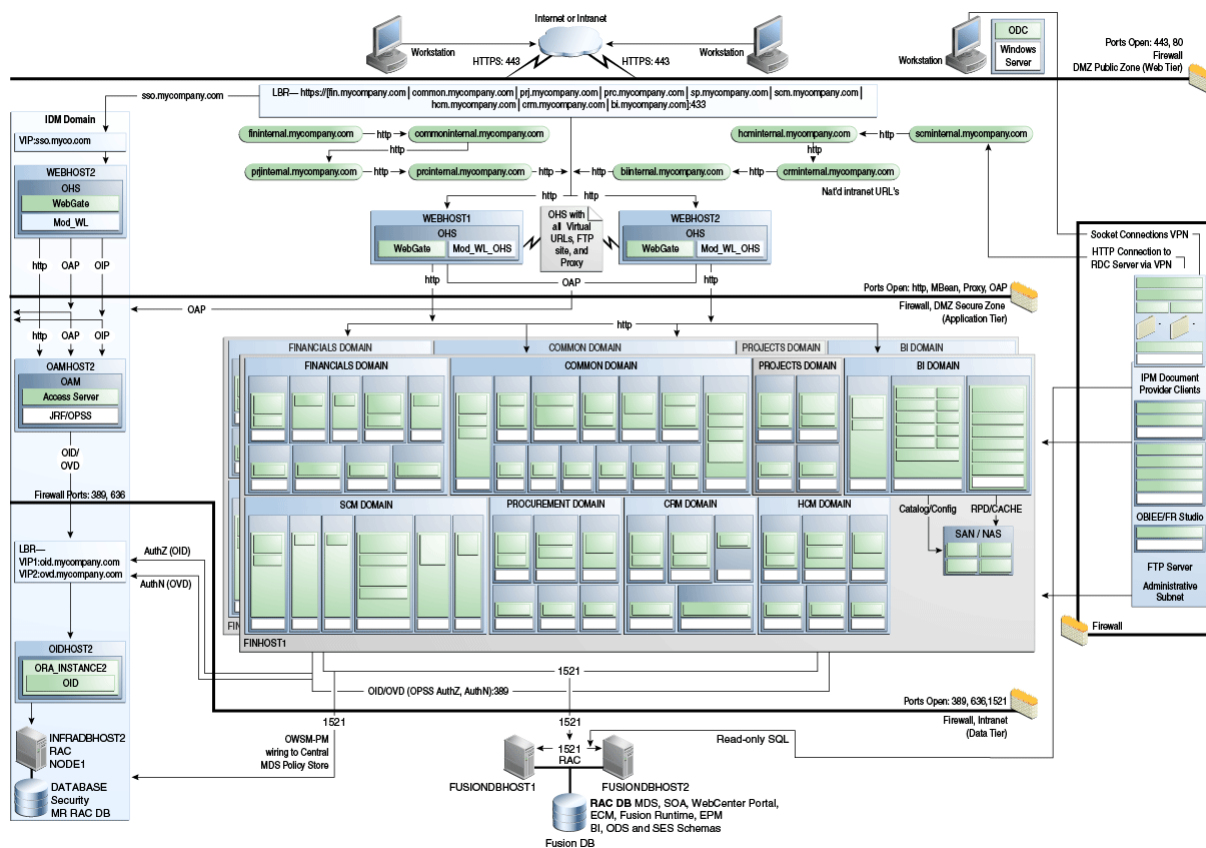
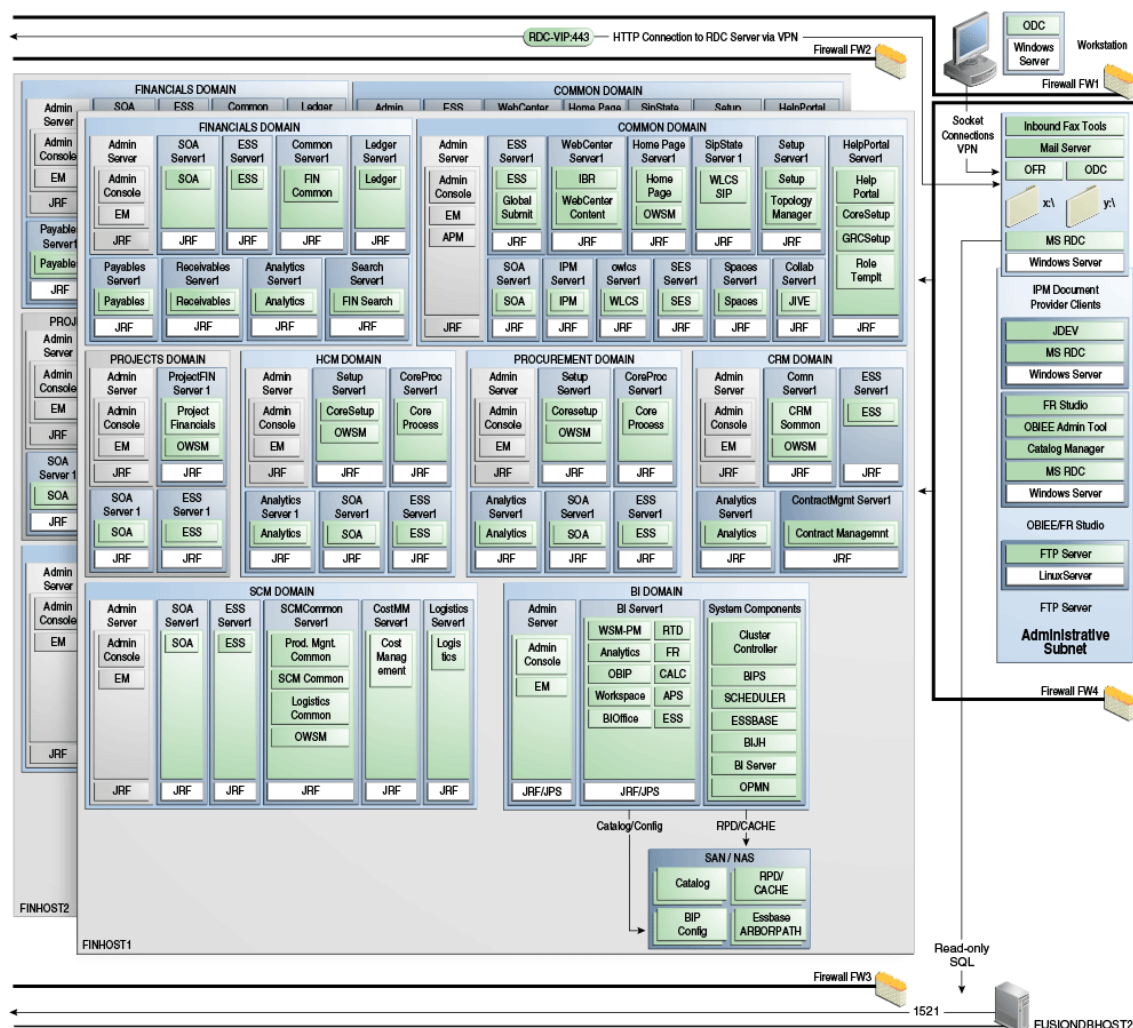


Figure A-2 Administrative Subnet Topology Details



A.2 Implementation

Implementing the administrative subnet requires the following:

- An RDC service enabled over HTTP and wired with a load-balancing router (LBR) virtual IP (VIP) running over HTTP Secure (HTTPS).
 - The LBR VIP should only be internal facing and use Secure Network Address Translation (SNAT) to enforce tighter security.
 - VPN must be used for clients that require socket connections.
- Different file systems created/mounted on the Windows server(s) using a universal naming convention (UNC) path and running the Oracle Forms Recognition and Oracle Document Capture clients.
 - An `x:\` directory, for example, where the Oracle Imaging and Process Management Linux input directory will be exposed over a Common Internet File System (CIFS) to the Windows server where Oracle Forms Recognition is running. (Oracle Imaging and Process Management needs read/write access to this file system; Oracle Forms Recognition needs only write access.)

- A `y:\` directory, for example, where Oracle Forms Recognition will write into the Oracle Imaging and Process Management input `x:\` directory. This is also the file system where Oracle Document Capture will write files to the import directory and Oracle Forms Recognition Runtime Server will read them on the Windows server. (Oracle Document Capture needs only write access to this file system; Oracle Forms Recognition needs read/write access.)
- An Oracle Forms Recognition batch directory, which needs to be exposed so that end users can correct data recognition problems using the OFR Verifier. This file system also needs to be exposed to OFR Designer.
 - * Because only a limited number of end users need OFR Verifier, it can be exposed through the remote desktop service (RDS).
 - * This file system is similar to the `y:\` file system topology.
- An Oracle Forms Recognition project directory, which needs to be exposed so that end users can modify Oracle Forms Recognition project configurations using OFR Designer.
 - * Because only a limited number of end users need OFR Designer, it can be exposed through the remote desktop service (RDS).
 - * This file system is similar to the `y:\` file system topology.

Certain accounts payable and accounts receivable situations have the following implementation requirements:

- A non-SSL Oracle Document Capture email server hosted in the administrative subnet to support the Oracle Fusion Expenses Oracle Document Capture email provider. Users in a customer network sends receipts through email attachments, the Oracle Document Capture email client processes the email attachments and drop them into the Oracle Imaging and Process Management input directory.
- The installation of a client-specific Oracle Document Capture at the customer location that will be integrated with their local scanners. There are two methods used to import scanned documents into the Oracle Forms Recognition import directory:
 - **Method 1:** By FTP. When receipts are scanned, Oracle Document Capture writes them locally. An automatic process will FTP the scanned documents into the Oracle Forms Recognition import directory.
 - **Method 2:** By file sharing. When receipts are scanned, Oracle Document Capture writes the scanned files into a remote input directory within the data center administrative subnet that is exposed to the customer network over VPN.

Oracle Forms Recognition reads and deletes the files and writes them into the Oracle Imaging and Process Management input directory, where they are read and further processed.

Method 1 is preferred because it does not expose the file system to the customer network.

- Access to a read-only Fusion database to allow Oracle Forms Recognition to query results.

Application administrators at a customer location must deploy applications from Oracle JDeveloper to an application server. This requires that the `APPLICATIONS_BASE` file system be mounted to the customer network. To implement the solution:

- Host Oracle JDeveloper on one of the Windows virtual machines within the administrative subnet. These Windows systems will access the client application administrators over the RDC with a VPN connection.

Mount the *APPLICATIONS_BASE* file system to this Windows virtual machine.

- Using the FTP server running in the administrative subnet, FTP application artifacts to the subnet and then deploy them through Oracle JDeveloper.

