

Oracle® Fusion Middleware

Administering Oracle Fusion Middleware

12c (12.1.3)

E48201-02

July 2014

Documentation for administrators that describes how to manage Oracle Fusion Middleware, including how to start and stop Oracle Fusion Middleware, how to configure and monitor components, and how to back up and recover your environment.

Oracle Fusion Middleware Administering Oracle Fusion Middleware, 12c (12.1.3)

E48201-02

Copyright © 2009, 2014, Oracle and/or its affiliates. All rights reserved.

Primary Author: Helen Grembowicz

Contributing Author: Vinaye Misra

Contributors: Mike Blevins, Nick Fry, Greg Cook, Harry Hsu, Christine Jacobs, Srinu Indla, Pavana Jain, Rama Kalava, Gopal Kirsur, Kenneth Ma, Dan MacKinnon, Manoj Nayak, Mark Nelson, Praveen Sampath, Sunita Sharma

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

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

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

U.S. GOVERNMENT RIGHTS Programs, software, databases, and related documentation and technical data delivered to U.S. Government customers are "commercial computer software" or "commercial technical data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, duplication, disclosure, modification, and adaptation shall be subject to the restrictions and license terms set forth in the applicable Government contract, and, to the extent applicable by the terms of the Government contract, the additional rights set forth in FAR 52.227-19, Commercial Computer Software License (December 2007). Oracle America, Inc., 500 Oracle Parkway, Redwood City, CA 94065.

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

Oracle 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	xxv
Audience	xxv
Documentation Accessibility	xxv
Related Documents	xxv
Conventions	xxvi
What's New in This Guide?	xxvii
New and Changed Features for Release 12c (12.1.3)	xxvii
New and Changed Features for Release 12c (12.1.2)	xxvii
Part I Understanding Oracle Fusion Middleware	
1 Introduction to Oracle Fusion Middleware	
1.1 What Is Oracle Fusion Middleware?	1-1
1.2 Oracle Fusion Middleware Components	1-1
Part II Basic Administration	
2 Getting Started Managing Oracle Fusion Middleware	
2.1 Overview of Oracle Fusion Middleware Administration Tools	2-1
2.2 Getting Started Using Oracle Enterprise Manager Fusion Middleware Control	2-3
2.2.1 Displaying Fusion Middleware Control	2-4
2.2.2 Using Fusion Middleware Control Help	2-4
2.2.3 Navigating Within Fusion Middleware Control	2-4
2.2.4 Understanding Users and Roles for Fusion Middleware Control	2-7
2.2.5 Viewing and Managing the WebLogic Domain	2-8
2.2.6 Viewing and Managing Components	2-9
2.3 Getting Started Using Oracle WebLogic Server Administration Console	2-10
2.3.1 Displaying the Oracle WebLogic Server Administration Console	2-11
2.3.2 Locking the WebLogic Server Configuration	2-11
2.4 Getting Started Using the Oracle WebLogic Scripting Tool (WLST)	2-12
2.4.1 Using WLST with Java Components	2-12
2.4.2 Using Custom WLST Commands	2-13
2.4.3 Using WLST Commands with System Components	2-13

2.5	Getting Started Using the Fusion Middleware Control MBean Browsers	2-15
2.5.1	Understanding MBeans	2-15
2.5.2	Using the System MBean Browser	2-15
2.5.3	Using the MBeans for a Selected Application	2-16
2.6	Changing the Administrative User Password	2-16
2.6.1	Changing the Administrative User Password Using the Command Line	2-17
2.6.2	Changing the Administrative User Password Using the Administration Console ..	2-17
2.7	Configuring Node Manager	2-17
2.7.1	Configuring Node Manager to Start Managed Servers	2-18
2.7.2	Configuring Node Manager to Use the OPSS Keystore Service	2-18
2.8	Basic Tasks for Configuring and Managing Oracle Fusion Middleware	2-19

3 Wiring Components to Work Together

3.1	Understanding Service Tables	3-1
3.2	Viewing Service Tables	3-1
3.3	Wiring Components Together	3-2
3.3.1	Wiring Oracle HTTP Server to the Administration Server	3-2
3.3.1.1	Why Wire Oracle HTTP Server to the Administration Server?	3-2
3.3.1.2	Connecting Oracle HTTP Server to the Administration Server	3-3
3.3.2	Routing Applications Through Oracle HTTP Server to Oracle WebLogic Server	3-4

4 Starting and Stopping Oracle Fusion Middleware

4.1	Overview of Starting and Stopping Procedures	4-1
4.2	Starting and Stopping Oracle WebLogic Server Administration and Managed Servers ..	4-1
4.2.1	Starting and Stopping Administration Server	4-2
4.2.2	Starting and Stopping Node Manager	4-2
4.2.3	Starting and Stopping Managed Servers	4-2
4.2.3.1	Starting and Stopping Managed Servers Using Fusion Middleware Control	4-2
4.2.3.2	Starting and Stopping Managed Servers Using Scripts	4-3
4.2.4	Enabling Servers to Start Without Supplying Credentials	4-3
4.2.5	Setting Up Oracle WebLogic Server as a Windows Service	4-4
4.3	Starting and Stopping Components	4-4
4.3.1	Starting and Stopping Components Using Fusion Middleware Control	4-4
4.3.2	Starting and Stopping Components Using the Command Line	4-5
4.3.2.1	Starting and Stopping Java Components	4-5
4.3.2.2	Starting and Stopping System Components	4-5
4.4	Starting and Stopping Fusion Middleware Control	4-6
4.5	Starting and Stopping Applications	4-6
4.5.1	Starting and Stopping Java EE Applications Using Fusion Middleware Control	4-7
4.5.2	Starting and Stopping Java EE Applications Using WLST	4-7
4.6	Starting and Stopping Your Oracle Fusion Middleware Environment	4-7
4.6.1	Starting an Oracle Fusion Middleware Environment	4-7
4.6.2	Stopping an Oracle Fusion Middleware Environment	4-8
4.7	Starting and Stopping: Special Topics	4-9
4.7.1	Starting and Stopping in High Availability Environments	4-9
4.7.2	Forcing a Shutdown of Oracle Database	4-9

5 Managing Ports

5.1	About Managing Ports	5-1
5.2	Viewing Port Numbers	5-1
5.2.1	Viewing Port Numbers Using the Command Line	5-1
5.2.2	Viewing Port Numbers Using Fusion Middleware Control	5-2
5.3	Changing the Port Numbers Used by Oracle Fusion Middleware	5-2
5.3.1	Changing the Oracle WebLogic Server Listen Ports	5-3
5.3.1.1	Changing the Oracle WebLogic Server Listen Ports Using the Administration Console	5-3
5.3.1.2	Changing the Oracle WebLogic Server Listen Ports Using WLST	5-3
5.3.2	Changing the Oracle HTTP Server Listen Ports	5-3
5.3.2.1	Enabling Oracle HTTP Server to Run as Root for Ports Set to Less Than 1024 (UNIX Only)	5-4
5.3.2.2	Changing the Oracle HTTP Server Non-SSL Listen Port in a WebLogic Server Domain	5-4
5.3.2.3	Changing the Oracle HTTP Server SSL Listen Port in a WebLogic Server Domain	5-4
5.3.2.4	Changing the Oracle HTTP Server Listen Ports in a Standalone Domain	5-5
5.3.3	Changing the Oracle Database Net Listener Port	5-5
5.3.3.1	Changing the KEY Value for an IPC Listener	5-6

Part III Secure Communication

6 Configuring SSL in Oracle Fusion Middleware

6.1	How SSL Works	6-1
6.1.1	What SSL Provides	6-2
6.1.2	About Private and Public Key Cryptography	6-2
6.1.3	Keystores and Wallets	6-3
6.1.4	How SSL Sessions Are Conducted	6-3
6.2	About SSL in Oracle Fusion Middleware	6-5
6.2.1	SSL in the Oracle Fusion Middleware Architecture	6-5
6.2.2	Keystores and Oracle Wallets	6-6
6.2.3	Authentication Modes	6-7
6.2.4	Tools for SSL Configuration	6-7
6.3	Configuring SSL for Configuration Tools	6-8
6.3.1	Oracle Enterprise Manager Fusion Middleware Control	6-8
6.3.2	Oracle WebLogic Server Administration Console	6-8
6.3.3	WLST Command-Line Tool	6-8
6.4	Configuring SSL for the Web Tier	6-9
6.4.1	Configuring Load Balancers	6-9
6.4.2	Enabling SSL for Oracle HTTP Server Virtual Hosts	6-9
6.4.2.1	Enabling SSL for Inbound Requests to Oracle HTTP Server Virtual Hosts Using Fusion Middleware Control	6-9
6.4.2.2	Enabling SSL for Inbound Requests to Oracle HTTP Server Virtual Hosts Using WLST	6-11
6.4.2.3	Enabling SSL for Outbound Requests from Oracle HTTP Server	6-12
6.4.2.3.1	Enabling One-Way SSL	6-12

6.4.2.3.2	Enabling Two-Way SSL	6-12
6.5	Configuring SSL for the Middle Tier	6-13
6.5.1	Configuring SSL for Oracle WebLogic Server	6-13
6.5.1.1	Configuring Inbound SSL to Oracle WebLogic Server	6-13
6.5.1.2	Configuring Outbound SSL from Oracle WebLogic Server	6-13
6.5.1.2.1	Configuring Outbound SSL from Oracle Platform Security Services to LDAP	6-14
6.5.1.2.2	Configuring Outbound SSL from Oracle Platform Security Services to Oracle Database	6-14
6.5.1.2.3	Configuring Outbound SSL from LDAP Authenticator to LDAP	6-14
6.5.1.2.4	Configuring Outbound SSL to the Database	6-14
6.5.2	Client-Side SSL for Applications	6-15
6.6	Configuring SSL for the Data Tier	6-15
6.6.1	Configuring SSL for the Database	6-15
6.6.1.1	SSL-Enabling Oracle Database	6-15
6.6.1.2	SSL-Enabling a Data Source	6-17
6.7	Advanced SSL Scenarios	6-18
6.7.1	Hardware Security Modules and Accelerators	6-18
6.7.2	CRL Integration with SSL	6-19
6.7.2.1	Configuring CRL Validation for a Component	6-20
6.7.2.2	Manage CRLs on the File System	6-20
6.7.2.3	Test a Component Configured for CRL Validation	6-21
6.7.3	Oracle Fusion Middleware FIPS 140-2 Settings	6-21
6.8	Best Practices for SSL	6-21
6.8.1	Best Practices for Administrators	6-22
6.8.2	Best Practices for Application Developers	6-22
6.9	WLST Reference for SSL	6-22

7 Managing Keystores, Wallets, and Certificates

7.1	Key and Certificate Storage in Oracle Fusion Middleware	7-1
7.1.1	Types of Keystores	7-1
7.1.1.1	About Oracle Wallet	7-1
7.1.1.2	About the JKS Keystore	7-2
7.1.1.3	About the Keystore Service (KSS) Keystore	7-2
7.1.2	Keystore Management Tools	7-2
7.2	Command-Line Interface for Keystores and Wallets	7-3
7.2.1	How to Launch the Command-Line Interface	7-3
7.3	Keystore Management	7-4
7.4	Wallet Management	7-4
7.4.1	About Wallets and Certificates	7-5
7.4.1.1	About Password-Protected and Autologin Wallets	7-5
7.4.1.2	About Self-Signed and Third-Party Wallets	7-6
7.4.1.3	Sharing Wallets Across Instances	7-6
7.4.1.4	Wallet Naming Conventions	7-6
7.4.1.5	Wallet Requirements in JDK7	7-7
7.4.2	Accessing the Wallet Management Page in Fusion Middleware Control	7-7
7.4.3	Managing the Wallet Life Cycle	7-7

7.4.4	Common Wallet Operations	7-8
7.4.4.1	Creating a Wallet	7-8
7.4.4.1.1	Creating a Wallet Using Fusion Middleware Control	7-8
7.4.4.1.2	Creating a Wallet Using WLST	7-9
7.4.4.2	Creating a Self-Signed Wallet	7-10
7.4.4.2.1	Creating a Self-Signed Wallet Using Fusion Middleware Control	7-10
7.4.4.2.2	Creating a Self-Signed Wallet Using WLST	7-11
7.4.4.3	Changing a Self-Signed Wallet to a Third-Party Wallet	7-11
7.4.4.4	Exporting a Wallet	7-11
7.4.4.4.1	Exporting a Wallet Using Fusion Middleware Control	7-11
7.4.4.4.2	Exporting a Wallet Using WLST	7-12
7.4.4.5	Importing a Wallet	7-12
7.4.4.5.1	Importing a Wallet Using Fusion Middleware Control	7-12
7.4.4.5.2	Importing a Wallet Using WLST	7-13
7.4.4.6	Deleting a Wallet	7-13
7.4.4.6.1	Deleting a Wallet Using Fusion Middleware Control	7-13
7.4.4.6.2	Deleting a Wallet Using WLST	7-14
7.4.5	Managing the Certificate Life Cycle	7-14
7.4.6	Accessing the Certificate Management Page for Wallets in Fusion Middleware Control	7-14
7.4.7	Common Certificate Operations	7-15
7.4.7.1	Adding a Certificate Request	7-15
7.4.7.1.1	Adding a Certificate Request Using Fusion Middleware Control	7-15
7.4.7.1.2	Adding a Certificate Request Using WLST	7-16
7.4.7.2	Exporting a Certificate, Certificate Request, or a Trusted Certificate	7-16
7.4.7.2.1	Exporting a Certificate, Certificate Request, or a Trusted Certificate Using Fusion Middleware Control	7-17
7.4.7.2.2	Exporting a Certificate, Certificate Request, or a Trusted Certificate Using WLST	7-17
7.4.7.3	Importing a Certificate or a Trusted Certificate	7-17
7.4.7.3.1	Importing a Certificate or a Trusted Certificate Using Fusion Middleware Control	7-17
7.4.7.3.2	Importing a Certificate or a Trusted Certificate Using WLST	7-18
7.4.7.4	Deleting a Certificate Request, a Certificate, or a Trusted Certificate	7-18
7.4.7.4.1	Deleting a Certificate Request, a Certificate, or a Trusted Certificate Using Fusion Middleware Control	7-18
7.4.7.4.2	Deleting a Certificate Request, a Certificate, or a Trusted Certificate Using WLST	7-19
7.4.7.5	Converting a Self-Signed Certificate into a Third-Party Certificate	7-19
7.4.7.5.1	Converting a Self-Signed Certificate into a Third-Party Certificate Using Fusion Middleware Control	7-19
7.4.7.5.2	Converting a Self-Signed Certificate into a Third-Party Certificate Using WLST	7-21
7.4.8	Wallet and Certificate Maintenance	7-22
7.4.8.1	Location of Wallets	7-22
7.4.8.2	Effect of Host Name Change on a Wallet	7-23
7.4.8.2.1	Requesting a New Certificate for a Production Wallet	7-23
7.4.8.2.2	Requesting a New Certificate for a Self-signed Wallet	7-23

7.4.8.3	Changing a Self-Signed Wallet to a Third-Party Wallet	7-23
7.4.8.4	Replacing an Expiring Certificate in a Wallet	7-24

8 FIPS 140 Support in Oracle Fusion Middleware

8.1	About the FIPS Standard	8-1
8.2	About FIPS 140 in Oracle Fusion Middleware Release 12c (12.1.3)	8-1
8.3	Components with FIPS 140 Support	8-3
8.4	Common Scenarios for an Operational FIPS 140 Environment	8-4
8.5	Troubleshooting FIPS 140 Issues	8-6
8.5.1	FIPS 140 Troubleshooting for Stand-alone WebLogic Server	8-6
8.5.2	FIPS 140 Troubleshooting for Oracle Platform Security Services	8-6
8.5.3	FIPS 140 Troubleshooting for Oracle Web Services Manager	8-7
8.5.4	FIPS 140 Troubleshooting for Database and JDBC Driver	8-7

Part IV Deploying Applications

9 Understanding the Deployment Process

9.1	What Is a Deployer?	9-1
9.2	General Procedures for Moving from Application Design to Production Deployment ...	9-1
9.2.1	Designing and Developing an Application	9-1
9.2.2	Deploying an Application to Managed Servers	9-2
9.2.3	Automating the Migration of an Application to Other Environments	9-4
9.3	Diagnosing Typical Problems	9-5

10 Deploying Applications

10.1	Overview of Deploying Applications	10-1
10.1.1	What Types of Applications Can You Deploy?	10-1
10.1.2	Understanding Deployment, Redeployment, and Undeployment	10-3
10.2	Understanding and Managing Data Sources	10-3
10.2.1	Understanding Data Sources	10-3
10.2.2	Creating and Managing JDBC Data Sources	10-4
10.2.2.1	Creating a JDBC Data Source Using Fusion Middleware Control	10-5
10.2.2.2	Editing a JDBC Data Source Using Fusion Middleware Control	10-6
10.2.2.3	Monitoring a JDBC Data Source Using Fusion Middleware Control	10-6
10.2.2.4	Controlling a JDBC Data Source Using Fusion Middleware Control	10-6
10.2.2.5	Creating a GridLink Data Source Using Fusion Middleware Control	10-7
10.3	Deploying, Undeploying, and Redeploying Java EE Applications	10-7
10.3.1	Deploying Java EE Applications	10-7
10.3.1.1	Deploying Java EE Applications Using Fusion Middleware Control	10-7
10.3.1.2	Deploying Java EE Applications Using WLST	10-10
10.3.2	Undeploying Java EE Applications	10-11
10.3.2.1	Undeploying Java EE Applications Using Fusion Middleware Control	10-11
10.3.2.2	Undeploying Java EE Applications Using WLST	10-12
10.3.3	Redeploying Java EE Applications	10-12
10.3.3.1	Redeploying Java EE Applications Using Fusion Middleware Control	10-12
10.3.3.2	Redeploying Java EE Applications Using WLST	10-14

10.4	Deploying, Undeploying, and Redeploying Oracle ADF Applications	10-14
10.4.1	Deploying Oracle ADF Applications	10-14
10.4.1.1	Deploying ADF Applications Using Fusion Middleware Control	10-14
10.4.1.2	Deploying ADF Applications Using WLST	10-18
10.4.1.3	Deploying ADF Applications Using the Administration Console	10-18
10.4.2	Undeploying Oracle ADF Applications	10-18
10.4.3	Redeploying Oracle ADF Applications	10-19
10.5	Deploying, Undeploying, and Redeploying SOA Composite Applications	10-21
10.5.1	Deploying SOA Composite Applications	10-21
10.5.2	Undeploying SOA Composite Applications	10-23
10.5.3	Redeploying SOA Composite Applications	10-23
10.6	Managing Deployment Plans	10-24
10.7	About the Common Deployment Tasks in Fusion Middleware Control	10-24
10.8	Changing MDS Configuration Attributes for Deployed Applications	10-26
10.8.1	Changing the MDS Configuration Attributes Using Fusion Middleware Control	10-27
10.8.2	Changing the MDS Configuration Using WLST	10-30
10.8.3	Restoring the Original MDS Configuration for an Application	10-31

Part V Monitoring Oracle Fusion Middleware

11 Monitoring Oracle Fusion Middleware

11.1	Monitoring the Status of Oracle Fusion Middleware	11-1
11.1.1	Monitoring an Oracle WebLogic Server Domain	11-2
11.1.2	Monitoring an Oracle WebLogic Server Administration or Managed Server	11-3
11.1.3	Monitoring a Cluster	11-3
11.1.4	Monitoring a Java Component	11-4
11.1.5	Monitoring a System Component	11-5
11.1.6	Monitoring Java EE Applications	11-6
11.1.7	Monitoring ADF Applications	11-7
11.1.8	Monitoring SOA Composite Applications	11-8
11.1.9	Monitoring Applications Deployed to a Cluster	11-9
11.1.10	Monitoring the Status of Components Using the Command Line	11-10
11.2	Viewing the Performance of Oracle Fusion Middleware	11-10
11.3	Viewing the Routing Topology	11-11

12 Managing Log Files and Diagnostic Data

12.1	Overview of Oracle Fusion Middleware Logging	12-1
12.1.1	Understanding Oracle Fusion Middleware HTTP Access Logging	12-1
12.1.2	Understanding Oracle Fusion Middleware Diagnostic Logging	12-2
12.2	Understanding ODL Messages and ODL Log Files	12-2
12.3	Viewing and Searching Log Files	12-5
12.3.1	Viewing Log Files and Their Messages	12-6
12.3.1.1	Viewing Log Files and Their Messages Using Fusion Middleware Control	12-6
12.3.1.2	Viewing Log Files and Their Messages Using WLST	12-7
12.3.2	Searching Log Files	12-9
12.3.2.1	Searching Log Files Using Fusion Middleware Control	12-9

12.3.2.1.1	Searching Log Files: Basic Searches	12-9
12.3.2.1.2	Searching Log Files: Advanced Searches	12-10
12.3.2.2	Searching Log Files Using WLST	12-11
12.3.3	Downloading Log Files	12-12
12.3.3.1	Downloading Log Files Using Fusion Middleware Control	12-13
12.3.3.2	Downloading Log Files for Specific Components Using Fusion Middleware Control	12-13
12.3.3.3	Downloading Specific Types of Messages Using Fusion Middleware Control	12-13
12.3.3.4	Downloading Log Files Using WLST	12-14
12.4	Configuring Settings for Log Files	12-14
12.4.1	Changing Log File Locations	12-15
12.4.1.1	Changing Log File Locations Using Fusion Middleware Control	12-15
12.4.1.2	Changing Log File Locations Using WLST	12-16
12.4.2	Configuring Log File Rotation	12-16
12.4.2.1	Specifying Log File Rotation Using Fusion Middleware Control	12-17
12.4.2.2	Specifying Log File Rotation Using WLST	12-18
12.4.3	Setting the Level of Information Written to Log Files	12-18
12.4.3.1	Configuring Message Levels Using Fusion Middleware Control	12-20
12.4.3.2	Configuring Message Levels Using WLST	12-21
12.4.4	Specifying the Log File Format	12-22
12.4.4.1	Specifying the Log File Format Using Fusion Middleware Control	12-22
12.4.4.2	Specifying the Log File Format Using WLST	12-22
12.4.5	Specifying the Log File Locale	12-22
12.4.5.1	Specifying the Log File Encoding Using WLST	12-23
12.4.5.2	Specifying the Log File Encoding in logging.xml	12-23
12.5	Correlating Messages Across Log Files and Components	12-23
12.6	Configuring Tracing	12-25
12.6.1	Configuring and Using QuickTrace	12-25
12.6.1.1	Understanding Quick Trace	12-25
12.6.1.2	Configuring QuickTrace	12-25
12.6.1.2.1	Configuring QuickTrace Using Fusion Middleware Control	12-26
12.6.1.2.2	Configuring QuickTrace Using WLST	12-27
12.6.1.3	Writing Trace Messages to a File	12-28
12.6.1.3.1	Writing the Trace Messages to a File Using Fusion Middleware Control	12-28
12.6.1.3.2	Writing the Trace Messages to a File Using WLST	12-29
12.6.1.4	Disabling QuickTrace Using WLST	12-29
12.6.2	Configuring and Using Selective Tracing	12-29
12.6.2.1	Understanding Selective Tracing	12-30
12.6.2.2	Configuring Selective Tracing	12-30
12.6.2.2.1	Configuring Selective Tracing Using Fusion Middleware Control	12-30
12.6.2.2.2	Configuring Selective Tracing Using WLST	12-32
12.6.2.3	Viewing Selective Traces	12-33
12.6.2.3.1	Viewing Selective Traces Using Fusion Middleware Control	12-33
12.6.2.3.2	Viewing Selective Traces Using WLST	12-34
12.6.2.4	Disabling Selective Tracing	12-34
12.6.2.4.1	Disabling Selective Tracing Using Fusion Middleware Control	12-34
12.6.2.4.2	Disabling Selective Traces Using WLST	12-34

13 Diagnosing Problems

13.1	Understanding the Diagnostic Framework	13-1
13.1.1	About Incidents and Problems	13-3
13.1.1.1	Incident Flood Control	13-3
13.1.2	Diagnostic Framework Components	13-3
13.1.2.1	Automatic Diagnostic Repository	13-4
13.1.2.2	Diagnostic Dumps	13-6
13.1.2.3	Management MBeans	13-6
13.1.2.4	WLST Commands for Diagnostic Framework	13-6
13.1.2.5	ADRCI Command-Line Utility	13-6
13.2	How the Diagnostic Framework Works	13-7
13.3	Configuring the Diagnostic Framework	13-9
13.3.1	Configuring Diagnostic Framework Settings	13-9
13.3.2	Configuring Custom Diagnostic Rules	13-12
13.3.3	Configuring Problem Suppression	13-15
13.3.4	Configuring WLDF Watch and Notification for the Diagnostic Framework	13-17
13.4	Investigating, Reporting, and Solving a Problem	13-19
13.4.1	Roadmap—Investigating, Reporting, and Resolving a Problem	13-20
13.4.2	Viewing Problems and Incidents	13-22
13.4.2.1	Viewing Problems	13-22
13.4.2.2	Viewing Incidents	13-23
13.4.2.3	Querying Incidents	13-23
13.4.3	Analyzing Specific Problem Keys	13-24
13.4.4	Working with Diagnostic Dumps	13-25
13.4.4.1	Listing Diagnostic Dumps	13-26
13.4.4.2	Viewing a Description of a Diagnostic Dump	13-27
13.4.4.3	Executing Dumps	13-27
13.4.5	Configuring and Using Diagnostic Dump Sampling	13-27
13.4.5.1	Understanding Diagnostic Dump Sampling	13-27
13.4.5.2	Configuring Dump Sampling	13-29
13.4.5.2.1	Activating the Default Samples	13-29
13.4.5.2.2	Creating Dump Samplings	13-30
13.4.5.2.3	Modifying Dump Sampling Settings	13-30
13.4.5.2.4	Removing Dump Samplings	13-30
13.4.5.2.5	Enabling or Disabling All Dump Sampling	13-30
13.4.5.3	Listing Dump Samplings	13-31
13.4.5.4	Retrieving the Dump Sampling Output	13-32
13.4.5.4.1	Retrieving Dump Samples Using the executeDump Command	13-32
13.4.5.4.2	Retrieving Dump Samples Using the getSamplingArchives Command ...	13-32
13.4.6	Managing Incidents	13-33
13.4.6.1	Creating an Incident Manually	13-33
13.4.6.2	Creating an Aggregated Incident	13-34
13.4.6.3	Packaging an Incident	13-35
13.4.6.4	Purging Incidents	13-37
13.4.7	Generating an RDA Report	13-37
13.5	Managing and Running the Health Test Framework	13-38
13.5.1	Understanding the Health Test Framework	13-39

13.5.2	Understanding the Health Test Framework File Repository	13-39
13.5.3	Using the Health Test Framework Command Line	13-39
13.5.3.1	dfwhealthtestadminctl.sh Command Line	13-39
13.5.3.1.1	help	13-40
13.5.3.1.2	register	13-40
13.5.3.1.3	index	13-41
13.5.3.2	dfwhealthtestctl.sh Command Line	13-41
13.5.3.2.1	desctest	13-41
13.5.3.2.2	help	13-42
13.5.3.2.3	listrun	13-42
13.5.3.2.4	listtest	13-42
13.5.3.2.5	report	13-42
13.5.3.2.6	run	13-43
13.5.3.2.7	status	13-44
13.5.4	Managing the Health Test Framework	13-44
13.5.4.1	Creating a Repository and Registering Health Test Framework Tests	13-44
13.5.4.2	Rebuilding the Health Test Framework Indexes	13-45
13.5.5	Running Health Test Framework Diagnostic Tests	13-45
13.5.6	Searching for Health Test Framework Diagnostic Tests	13-46
13.5.7	Retrieving a Description of a Health Test Framework Test	13-47
13.5.8	Listing Health Test Framework Test Runs	13-47
13.5.9	Generating Health Test Framework Reports	13-47

Part VI Advanced Administration

14 Managing the Metadata Repository

14.1	Understanding a Metadata Repository	14-1
14.2	Creating a Database-Based Metadata Repository	14-2
14.3	Managing the MDS Repository	14-2
14.3.1	Understanding the MDS Repository	14-3
14.3.1.1	Databases Supported by MDS	14-4
14.3.1.2	Understanding MDS Operations	14-5
14.3.2	Registering and Deregistering a Database-Based MDS Repository	14-6
14.3.2.1	Registering a Database-Based MDS Repository	14-7
14.3.2.1.1	Registering a Database-Based MDS Repository Using Fusion Middleware Control	14-7
14.3.2.1.2	Registering a Database-Based MDS Repository Using WLST	14-9
14.3.2.2	Adding or Removing Servers Targeted to the MDS Repository	14-9
14.3.2.3	Deregistering a Database-Based MDS Repository	14-11
14.3.2.3.1	Deregistering a Database-Based MDS Repository Using Fusion Middleware Control	14-11
14.3.2.3.2	Deregistering a Database-Based MDS Repository Using WLST	14-11
14.3.3	Registering and Deregistering a File-Based MDS Repository	14-11
14.3.3.1	Creating and Registering a File-Based MDS Repository	14-12
14.3.3.2	Deregistering a File-Based MDS Repository	14-13
14.3.4	Changing the System Data Source	14-13
14.3.5	Using System MBeans to Manage an MDS Repository	14-13

14.3.6	Viewing Information About an MDS Repository	14-14
14.3.6.1	Viewing Information About an MDS Repository Using Fusion Middleware Control	14-14
14.3.6.2	Viewing Information About an MDS Repository Using System MBeans	14-15
14.3.7	Configuring an Application to Use a Different MDS Repository or Partition	14-15
14.3.7.1	Cloning a Partition	14-16
14.3.7.2	Creating a New Partition and Reassociating the Application to It	14-18
14.3.8	Moving Metadata from a Source System to a Target System	14-18
14.3.8.1	Transferring Metadata Using Fusion Middleware Control	14-19
14.3.8.2	Transferring Metadata using WLST	14-20
14.3.9	Moving from a File-Based Repository to a Database-Based Repository	14-21
14.3.10	Deleting a Metadata Partition from a Repository	14-21
14.3.10.1	Deleting a Metadata Partition Using Fusion Middleware Control	14-22
14.3.10.2	Deleting a Metadata Partition Using WLST	14-22
14.3.11	Purging Metadata Version History	14-22
14.3.11.1	Purging Metadata Version History Using Fusion Middleware Control	14-22
14.3.11.2	Purging Metadata Version History Using WLST	14-23
14.3.11.3	Enabling Auto-Purge	14-23
14.3.12	Managing Metadata Labels in the MDS Repository	14-23
14.3.12.1	Creating Metadata Labels	14-24
14.3.12.2	Listing Metadata Labels	14-24
14.3.12.3	Promoting Metadata Labels	14-24
14.3.12.4	Purging Metadata Labels	14-25
14.3.12.4.1	Purging Metadata Labels Using Fusion Middleware Control	14-25
14.3.12.4.2	Purging Metadata Labels Using WLST	14-27
14.3.12.5	Deleting Metadata Labels	14-27
14.4	Managing Metadata Repository Schemas	14-27
14.4.1	Changing Metadata Repository Schema Passwords	14-27
14.4.1.1	Changing the Schema Passwords for Most Components	14-28
14.4.1.2	Changing the Schema Password for Oracle Platform Security Services	14-28
14.4.2	Changing the Character Set of the Metadata Repository	14-29
14.5	Purging Data	14-29
14.5.1	Purging Oracle Infrastructure Web Services Data	14-31

15 Changing Network Configurations

15.1	Changing the Network Configuration of Oracle Fusion Middleware	15-1
15.1.1	Changing the Network Configuration of an Administration Server	15-1
15.1.2	Changing the Network Configuration of a Managed Server	15-2
15.1.3	Changing the Network Configuration of Oracle HTTP Server	15-3
15.2	Changing the Network Configuration of a Database	15-3
15.3	Moving Between On-Network and Off-Network	15-6
15.3.1	Moving from Off-Network to On-Network (Static IP Address)	15-6
15.3.2	Moving from Off-Network to On-Network (DHCP)	15-6
15.3.3	Moving from On-Network to Off-Network (Static IP Address)	15-6
15.4	Changing Between a Static IP Address and DHCP	15-6
15.4.1	Changing from a Static IP Address to DHCP	15-7
15.4.2	Changing from DHCP to a Static IP Address	15-7

15.5	Using IPv6	15-7
15.5.1	Configuring Oracle HTTP Server for IPv6	15-7
15.5.2	Using Dual Stack with Oracle SOA Suite and Fusion Middleware Control	15-8

Part VII Advanced Administration: Backup and Recovery

16 Introducing Backup and Recovery

16.1	Understanding Oracle Fusion Middleware Backup and Recovery	16-1
16.1.1	Impact of Administration Server Failure	16-2
16.1.2	Managed Server Independence (MSI) Mode	16-2
16.1.3	Configuration Changes in Managed Servers	16-2
16.2	Oracle Fusion Middleware Directory Structure	16-3
16.3	Tools to Use for Backup and Recovery	16-3
16.4	Backup and Recovery Recommendations for Oracle Fusion Middleware Components	16-4
16.4.1	Backup and Recovery Considerations for Oracle WebLogic Server JMS	16-7
16.4.2	Backup and Recovery Recommendations for Oracle BPEL Process Manager	16-9
16.5	Assumptions and Restrictions	16-9

17 Backing Up Your Environment

17.1	Overview of the Backup Strategies	17-1
17.1.1	Types of Backups	17-1
17.1.2	Backup Artifacts	17-2
17.1.3	Recommended Backup Strategy	17-2
17.2	Limitations and Restrictions for Backing Up Data	17-4
17.3	Performing a Backup	17-5
17.3.1	Performing a Full Offline Backup	17-5
17.3.2	Performing an Online Backup of Run-Time Artifacts	17-6
17.3.3	Backing Up Windows Registry Entries	17-7
17.4	Creating a Record of Your Oracle Fusion Middleware Configuration	17-7

18 Recovering Your Environment

18.1	Overview of Recovery Strategies	18-1
18.1.1	Types of Recovery	18-1
18.1.2	Recommended Recovery Strategies	18-2
18.2	Recovering After Data Loss, Corruption, Media Failure, or Application Malfunction ..	18-3
18.2.1	Recovering the Oracle Home	18-4
18.2.2	Recovering an Oracle WebLogic Server Domain	18-4
18.2.2.1	Recovering Oracle WebLogic Server with Whole Server Migration	18-5
18.2.3	Recovering a Standalone Domain	18-5
18.2.4	Recovering the Administration Server Configuration	18-5
18.2.5	Recovering a Managed Server	18-6
18.2.6	Recovering a Component	18-7
18.2.6.1	Recovering Oracle Platform Security Services	18-8
18.2.6.2	Recovering Oracle B2B	18-8
18.2.7	Recovering a Cluster	18-8
18.2.8	Recovering Applications	18-9

18.2.8.1	Recovering Application Artifacts	18-9
18.2.8.2	Recovering a Java EE Application	18-9
18.2.9	Recovering a Database	18-10
18.3	Recovering After Loss of Host	18-10
18.3.1	Recovering After Loss of Oracle WebLogic Server Domain Host	18-10
18.3.2	Recovering After Loss of Standalone Domain Host	18-10
18.3.2.1	Recovering a Standalone Domain to the Same Host	18-11
18.3.2.2	Recovering a Standalone Domain to a Different Host	18-11
18.3.3	Recovering After Loss of Administration Server Host	18-11
18.3.3.1	Recovering the Administration Server to the Same Host	18-12
18.3.3.2	Recovering the Administration Server to a Different Host	18-12
18.3.4	Recovering After Loss of Managed Server Host	18-14
18.3.4.1	Recovering a Managed Server to the Same Host	18-14
18.3.4.2	Recovering a Managed Server to a Different Host	18-15
18.3.5	Recovering After Loss of Component Host	18-17
18.3.5.1	Recovering a Java Component to the Same or Different Host	18-18
18.3.5.2	Recovering a Java Component to a Different Host	18-18
18.3.5.3	Recovering a System Component to the Same or Different Host	18-18
18.3.5.4	Recovering Oracle SOA Suite After Loss of Host	18-18
18.3.5.5	Recovering Web Tier Components to a Different Host	18-19
18.3.5.5.1	Recovering Oracle HTTP Server in a Standalone Domain to a Different Host	18-19
18.3.5.5.2	Recovering Oracle HTTP Server in a WebLogic Server Domain to a Different Host	18-19
18.3.5.6	Recovering Oracle Data Integrator to a Different Host	18-20
18.3.5.6.1	Recovering Oracle Data Integrator Repository	18-20
18.3.5.6.2	Recovering Oracle Data Integrator Agents to a Different Host	18-21
18.3.6	Additional Actions for Recovering Entities After Loss of Host	18-21
18.3.6.1	Recovering Fusion Middleware Control to a Different Host	18-21
18.3.6.2	Modifying the mod_wl_ohs.conf File	18-22
18.3.6.3	Creating a New Machine for Certain Components	18-22
18.3.6.4	Updating Oracle Inventory	18-23
18.3.6.5	Recovering the Windows Registry	18-23
18.3.7	Recovering After Loss of Database Host	18-24

Part VIII Advanced Administration: Expanding Your Environment

19 Scaling Up Your Environment

19.1	Overview of Scaling Up Your Environment	19-1
19.2	Extending a Domain to Support Additional Components	19-2
19.3	Adding Additional Managed Servers to a Domain	19-3
19.3.1	Applying Oracle JRF Template to a Managed Server or Cluster	19-4
19.4	Creating Clusters	19-6
19.5	Creating a Standalone Domain and a System Component	19-7
19.6	Creating a System Component Instance in a WebLogic Server Domain	19-7
19.7	Copying an Oracle Home or Component	19-8

20 Moving from a Test to a Production Environment

20.1	Introduction to Moving Oracle Fusion Middleware Components	20-1
20.2	Planning for Moving Your Environment	20-2
20.2.1	Introduction to the Movement Scripts	20-2
20.2.2	Checking the Source Environment	20-3
20.2.3	Understanding How the Movement Scripts Work with Keystores	20-4
20.2.4	Preparing the Target Environment	20-5
20.2.5	Limitations in Moving from Source to Target	20-6
20.2.6	Overview of Procedures for Moving from a Source to a Target Environment	20-7
20.3	Common Procedures for Moving to a Target Environment	20-9
20.3.1	Installing the Database on the Target Environment	20-10
20.3.2	Moving the Oracle Home and the Binary Files Using the Scripts	20-10
20.3.3	Moving the Oracle Home and Binary Files Using Storage-Level Cloning Tools ...	20-12
20.3.4	Moving the Configuration of a WebLogic Server Domain	20-13
20.3.5	Moving the Configuration of a Standalone Domain	20-15
20.3.6	Moving the Configuration of Node Manager	20-16
20.3.7	Configuring Users and Groups	20-18
20.3.8	Starting Managed Servers and Components	20-18
20.4	Additional Steps or Information for Certain Components	20-18
20.4.1	Additional Steps for Moving Oracle Data Integrator	20-19
20.4.2	Additional Steps for Moving Oracle B2B	20-21
20.4.3	Additional Steps for Moving Oracle Business Process Management	20-22
20.5	Incrementally Moving Artifacts	20-24
20.6	Moving Distributed Topologies	20-24
20.6.1	Considerations with a Multiple Host Environment	20-24
20.6.2	Considerations in Moving to and from an Oracle RAC Environment	20-25
20.7	Recovering from Test to Production Errors	20-26

Part IX Appendixes

A Movement Scripts and Move Plans

A.1	Understanding the Movement Scripts	A-1
A.1.1	Specifying Java Options	A-3
A.1.2	Movement Scripts Syntax	A-4
A.1.2.1	copyBinary Script	A-5
A.1.2.2	pasteBinary Script	A-6
A.1.2.3	copyConfig Script for Oracle WebLogic Server Domains	A-8
A.1.2.4	copyConfig Script for Standalone Domains	A-10
A.1.2.5	copyConfig Script for Node Manager	A-12
A.1.2.6	extractMovePlan Script	A-13
A.1.2.7	pasteConfig Script for Oracle WebLogic Server Domains	A-14
A.1.2.8	pasteConfig Script for Standalone Domains	A-16
A.1.2.9	pasteConfig Script for Node Manager	A-17
A.1.2.10	obfuscatePassword Script and API	A-19
A.2	Modifying Move Plans	A-19
A.2.1	Locating configGroup Elements	A-20

A.2.2	Move Plan Properties	A-21
-------	----------------------------	------

B Oracle Fusion Middleware Command-Line Tools

C URLs for Components

D Port Numbers

D.1	Port Numbers by Component	D-1
D.2	Port Numbers (Sorted by Number)	D-2

E Using Oracle Fusion Middleware Accessibility Options

E.1	Install and Configure Java Access Bridge (Windows Only)	E-1
E.2	Enabling Fusion Middleware Control Accessibility Mode	E-1
E.2.1	Making HTML Pages More Accessible	E-2
E.2.2	Viewing Text Descriptions of Fusion Middleware Control Charts	E-3
E.3	Fusion Middleware Control Keyboard Navigation	E-3

F Viewing Release Numbers

F.1	Release Number Format	F-1
F.2	Viewing the Software Inventory and Release Numbers	F-2
F.2.1	Viewing Oracle Fusion Middleware Installation Release Numbers	F-2
F.2.2	Viewing Oracle WebLogic Server Release Numbers	F-2
F.2.3	Viewing Component Release Numbers	F-3
F.2.4	Viewing Metadata Repository Release Numbers	F-3
F.2.5	Viewing Schema Release Numbers	F-3

G orapki

G.1	Using the orapki Utility for Certificate and CRL Management	G-1
G.1.1	orapki Overview	G-2
G.1.1.1	orapki Syntax	G-2
G.1.1.2	Environment Setup for orapki	G-3
G.1.2	Displaying orapki Help	G-3
G.1.3	Creating Signed Certificates for Testing Purposes	G-3
G.1.4	Managing Oracle Wallets with the orapki Utility	G-3
G.1.4.1	Creating and Viewing Oracle Wallets with orapki	G-4
G.1.4.1.1	Creating an Oracle Wallet	G-4
G.1.4.1.2	Creating an Oracle Wallet with Auto-login Enabled	G-4
G.1.4.1.3	Creating an Oracle Wallet with AES Encryption	G-4
G.1.4.1.4	Converting an Existing Wallet to Use AES Encryption	G-4
G.1.4.1.5	Viewing an Oracle Wallet	G-4
G.1.4.2	Adding Certificates and Certificate Requests to Oracle Wallets with orapki	G-5
G.1.4.2.1	Adding a Certificate Request to an Oracle Wallet	G-5
G.1.4.2.2	Adding a Trusted Certificate to an Oracle Wallet	G-5
G.1.4.2.3	Adding a Root Certificate to an Oracle Wallet	G-5
G.1.4.2.4	Adding a User Certificate to an Oracle Wallet	G-6

G.1.4.3	Exporting Certificates and Certificate Requests from Oracle Wallets with orapki	G-6
G.1.4.3.1	Exporting a Certificate from an Oracle Wallet	G-6
G.1.4.3.2	Exporting a Certificate Request from an Oracle Wallet	G-6
G.1.4.4	Creating and Managing Trust Flags	G-6
G.1.4.4.1	Creating a Wallet to Support Trust Flags	G-7
G.1.4.4.2	Converting a Wallet to Support Trust Flags	G-8
G.1.4.4.3	Adding and Updating a Certificate's Trust Flags	G-8
G.1.4.4.4	Adding a Certificate with Trust Flags to Wallet	G-9
G.1.4.5	Importing PKCS#12 Files to an Oracle Wallet	G-9
G.1.5	Managing Certificate Revocation Lists (CRLs) with orapki Utility	G-9
G.1.5.1	About Certificate Validation with Certificate Revocation Lists	G-10
G.1.5.1.1	What CRLs Should You Use?	G-10
G.1.5.1.2	How CRL Checking Works	G-10
G.1.5.2	Certificate Revocation List Management	G-11
G.1.5.2.1	Renaming CRLs with a Hash Value for Certificate Validation	G-11
G.1.6	orapki Utility Commands Summary	G-12
G.1.6.1	orapki cert create	G-12
G.1.6.1.1	Purpose	G-12
G.1.6.1.2	Syntax	G-12
G.1.6.2	orapki cert display	G-13
G.1.6.2.1	Purpose	G-13
G.1.6.2.2	Syntax	G-13
G.1.6.3	orapki crl create	G-13
G.1.6.3.1	Purpose	G-13
G.1.6.3.2	Syntax	G-13
G.1.6.4	orapki crl hash	G-13
G.1.6.4.1	Purpose	G-13
G.1.6.4.2	Syntax	G-13
G.1.6.5	orapki crl revoke	G-14
G.1.6.5.1	Purpose	G-14
G.1.6.5.2	Syntax	G-14
G.1.6.6	orapki crl status	G-14
G.1.6.6.1	Purpose	G-14
G.1.6.6.2	Syntax	G-14
G.1.6.7	orapki crl verify	G-14
G.1.6.7.1	Purpose	G-14
G.1.6.7.2	Syntax	G-14
G.1.6.8	orapki wallet add	G-15
G.1.6.8.1	Purpose	G-15
G.1.6.8.2	Syntax	G-15
G.1.6.9	orapki wallet change_pwd	G-16
G.1.6.9.1	Purpose	G-16
G.1.6.9.2	Syntax	G-16
G.1.6.10	orapki wallet create	G-16
G.1.6.10.1	Purpose	G-16
G.1.6.10.2	Syntax	G-16
G.1.6.11	orapki wallet enable_trust_flags	G-16

G.1.6.11.1	Purpose	G-16
G.1.6.11.2	Syntax	G-16
G.1.6.12	orapki wallet assign_trust_flags	G-17
G.1.6.12.1	Purpose	G-17
G.1.6.12.2	Syntax	G-17
G.1.6.13	orapki wallet display	G-17
G.1.6.13.1	Purpose	G-17
G.1.6.13.2	Syntax	G-17
G.1.6.14	orapki wallet export	G-17
G.1.6.14.1	Purpose	G-17
G.1.6.14.2	Syntax	G-17
G.1.6.15	orapki wallet export_trust_chain	G-18
G.1.6.15.1	Purpose	G-18
G.1.6.15.2	Syntax	G-18
G.1.6.16	orapki wallet import_pkcs12	G-18
G.1.6.16.1	Purpose	G-18
G.1.6.16.2	Syntax	G-18

H Troubleshooting Oracle Fusion Middleware

H.1	Diagnosing Oracle Fusion Middleware Problems	H-1
H.2	Common Problems and Solutions	H-1
H.2.1	Running out of Data Source Connections	H-2
H.2.2	Using a Different Version of Spring	H-2
H.2.3	ClassNotFoundException Errors When Starting Managed Servers	H-2
H.3	Troubleshooting SSL	H-2
H.3.1	Components May Enable All Supported Ciphers	H-3
H.3.2	SSL Certificate Chain Required on Certain Browsers	H-3
H.3.3	keyUsage Extension Required for Certificates in JDK7	H-3
H.4	Troubleshooting FIPS Configuration	H-4
H.5	Need More Help?	H-4
H.5.1	Using Remote Diagnostic Agent	H-4

List of Figures

6-1	SSL Handshake.....	6-5
6-2	SSL in Oracle Fusion Middleware	6-5
8-1	Selecting a FIPS 140 Provider	8-3
13-1	ADR Directory Structure for Oracle Fusion Middleware	13-5
13-2	Incident Creation Generated by Incident Log Detector	13-7
13-3	Incident Creation Generated by WLDF Watch Notification	13-8
13-4	Flow for Investigating a Problem	13-21
17-1	Decision Flow Chart for Type of Backup	17-4
20-1	Flowchart for Moving Your Environment	20-8
F-1	Example of an Oracle Fusion Middleware Release Number.....	F-1

List of Tables

2-1	Comparing Fusion Middleware Control and WebLogic Server Administration Console	2-2
2-2	Navigating Within Fusion Middleware Control.....	2-6
2-3	Roles Supported by Fusion Middleware Control	2-7
2-4	Privileges for the Supported Roles	2-7
2-5	WLST Commands for System Components	2-14
7-1	Keystore Types in Oracle Fusion Middleware	7-1
8-1	Components with FIPS 140 Support in Oracle Fusion Middleware	8-4
8-2	FIPS 140 Scenarios.....	8-5
9-1	Oracle JDeveloper Extensions	9-4
10-1	Tools to Deploy Applications.....	10-2
10-2	MDS Configuration Attributes for Deployed Applications	10-28
12-1	ODL Format Message Fields	12-3
12-2	Log File Location for Oracle Fusion Middleware Components.....	12-4
12-3	Diagnostic Message Types and Level	12-18
12-4	Mapping of Log Levels Among ODL, Oracle WebLogic Server, and Java	12-19
13-1	DiagnosticConfig MBean Attributes for Diagnostic Framework	13-10
13-2	Conditions for the LogDetectionConditions Element	13-13
13-3	Optional arguments for the defaultActions Element	13-14
13-4	Attributes for the ruleCondition Element	13-14
13-5	DiagnosticConfig MBean Operations and Attributes for Problem Suppression Filters	13-16
13-6	Uncaught Exception Problem Keys.....	13-25
13-7	Diagnostic Dump Actions.....	13-26
13-8	Default Diagnostic Dump Samplings Configuration	13-28
13-9	Health Test Framework dfwhealthtestadminctl.sh Commands.....	13-40
13-10	Health Test Framework dfwhealthtestctl.sh Commands	13-41
14-1	MDS Operations and Required Roles	14-5
14-2	Purging Data Documentation	14-30
16-1	Backup and Recovery Recommendations.....	16-5
18-1	Additional Recovery Procedures for Particular Components.....	18-3
20-1	Support for Movement Scripts.....	20-3
20-2	Components Requiring Additional Steps for Movement to a Different Environment.....	20-18
A-1	Movement Scripts	A-1
A-2	Options for the copyBinary Script	A-5
A-3	Options for the pasteBinary Script	A-7
A-4	Options for the copyConfig Script for Oracle WebLogic Server Domains.....	A-9
A-5	Options for the copyConfig Script for Standalone Domains.....	A-11
A-6	Options for the copyConfig Script for Node Manager.....	A-12
A-7	Options for the extractMovePlan Script	A-14
A-8	Options for the pasteConfig Script for Oracle WebLogic Server Domains.....	A-15
A-9	Options for the pasteConfig Script for Standalone Domains	A-17
A-10	Options for the pasteConfig Script for Node Manager	A-18
A-11	Move Plan Properties for Components	A-21
A-12	Move Plan Properties for Node Manager in a Standalone Domain.....	A-22
A-13	Common Move Plan Properties for Java Components	A-23
A-14	Move Plan Properties for Oracle ADF Connections	A-31
A-15	Move Plan Properties for Oracle Coherence.....	A-33
A-16	Move Plan Properties for Oracle Web Services Manager	A-34
A-17	Move Plan Properties for Oracle HTTP Server.....	A-36
A-18	Move Plan Properties for Oracle SOA Suite	A-38
A-19	Move Plan Properties for Oracle Business Activity Monitoring.....	A-38

A-20	Move Plan Properties for SOA Core Extensions	A-39
A-21	Move Plan Properties for Oracle Service Bus	A-39
A-22	Move Plan Properties for Oracle User Messaging Service.....	A-40
A-23	Move Plan Properties for Oracle B2B.....	A-42
A-24	Move Plan Properties for Oracle Enterprise Scheduler.....	A-45
A-25	Move Plan Properties for Oracle Managed File Transfer.....	A-46
A-26	Move Plan Properties for Oracle Data Integrator	A-47
B-1	Oracle Fusion Middleware Command-Line Tools	B-1
C-1	URLs for Components.....	C-1
D-1	Port Numbers Sorted by Component	D-1
D-2	Port Numbers Sorted by Number	D-2
E-1	Keyboard Navigation for Common Tasks	E-4
E-2	Keyboard Navigation for Topology Viewer	E-4
G-1	Trust Flags in Oracle Wallet Certificates	G-6

Preface

This guide describes how to manage Oracle Fusion Middleware, including how to start and stop Oracle Fusion Middleware, how to change ports, deploy applications, how to back up and recover Oracle Fusion Middleware and how to move your environment from a source environment, such as a test environment to a target environment, such as a production environment.

Audience

This guide is intended for administrators of Oracle Fusion Middleware.

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 Middleware 12c (12.1.3) documentation set:

- *Understanding Oracle Fusion Middleware*
- *Securing Applications with Oracle Platform Security Services*
- *High Availability Guide*
- *Understanding Oracle WebLogic Server*
- *Tuning Performance*
- *Administering Oracle SOA Suite and Oracle Business Process Management Suite*
- *Administering Oracle HTTP Server*
- *Administering Web Services*

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.
monospace	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

What's New in This Guide?

This preface introduces the new and changed administrative features of Oracle Fusion Middleware that are described in this guide, and provides pointers to additional information.

New and Changed Features for Release 12c (12.1.3)

The following topics introduce the new and changed features of Oracle Fusion Middleware and other significant changes that are described or referred to in this guide, and provides pointers to additional information.

- Node Manager support for the OPSS Keystore Service. See [Section 2.7.2](#) for information about configuring Node Manager.
- Revised support for moving the OPSS Keystore Service to a new environment. See [Section 20.2.3](#). Also see [Table A-13](#) for move plan properties related to the Keystore Service.
- Support for moving the following components to a new environment:
 - Oracle User Messaging Service. See [Table A-22](#) for the move plan properties.
 - Oracle Managed File Transfer. See [Table A-25](#) for the move plan properties.
 - Oracle SOA Core Extensions. See [Table A-20](#) for the move plan properties.
 - Oracle Enterprise Data Quality, which uses the move plan properties for Java components. See [Table A-13](#).

See [Table 20-1](#) for a complete list of components that support the movement scripts.

- Enhanced move plan properties for Oracle B2B. See [Table A-23](#).
- Support for AES encryption for Oracle Wallets. See [Section G.1.4.1.3](#) and [Section G.1.4.1.4](#).
- Support for certificate trust flags in Oracle Wallets. See [Section G.1.4.4](#).
- Ability to import PKCS#12 files to Oracle Wallet. See [Section G.1.4.5](#).
- FIPS-140 support in Oracle Fusion Middleware. See [Chapter 8](#).

New and Changed Features for Release 12c (12.1.2)

The following topics introduce the new and changed features of Oracle Fusion Middleware and other significant changes that are described or referred to in this

guide, and provides pointers to additional information. This book is the new edition of the formerly titled *Oracle Fusion Middleware Administrator's Guide*.

- Redefining of the Oracle home and elimination of the Middleware home. See "New And Deprecated Terminology for 12c" in *Understanding Oracle Fusion Middleware*.
- OPMN is no longer used in Oracle Fusion Middleware. Instead, system components are managed by the WebLogic Management Framework, which includes WLST, Node Manager and pack and unpack. See "What Is the WebLogic Management Framework" in *Understanding Oracle Fusion Middleware*.
- Support for a "per domain" Node Manager. See "What Is Node Manager?" in *Understanding Oracle Fusion Middleware*.
- Oracle Web Cache is no longer part of Oracle Fusion Middleware.
- Changes in moving from a source to a target environment:
 - Because of the redefining of Oracle home and elimination of Middleware home, some of the parameters to the scripts have changed. See [Section A.1.2](#).
 - Support for moving a standalone domain. See [Section 20.3.5](#).
 - Support for moving the Oracle home and binary files using storage-level cloning tools. See [Section 20.3.3](#).
 - A move plan for Oracle Coherence. See [Table A–15](#).
 - A move plan for Oracle Web Services Manager. See [Table A–16](#).
- The OPSS Keystore Service is introduced. See [Section 7.1.1.3](#).
- SSL procedures for Oracle WebLogic Server have been updated. See [Section 6.5.1](#).
- Fusion Middleware Control supports cross-component wiring. See [Section 3.3](#).
- Oracle Fusion Middleware has introduced service tables, which provide a way for service providers to publish endpoint information about their services, and clients of these services to query and bind to these services. See [Section 3.1](#).
- Updated procedures for backup and recovery, including procedures for recovering a standalone domain. See [Chapter 18](#).
- Enhanced support for querying diagnostic incidents. See [Section 13.4.2.3](#).
- Support for creating aggregated incidents. See [Section 13.4.6.2](#).
- Support for extended log format for access logs. See [Section 12.1.1](#).

Part I

Understanding Oracle Fusion Middleware

This part provides an overview to Oracle Fusion Middleware and its concepts as they relate to administering Oracle Fusion Middleware.

[Part I](#) contains the following chapter:

- [Chapter 1, "Introduction to Oracle Fusion Middleware"](#)

Introduction to Oracle Fusion Middleware

Oracle Fusion Middleware is a comprehensive family of products ranging from application development tools and integration solutions to identity management, collaboration, and business intelligence reporting. This chapter provides an introduction to Oracle Fusion Middleware.

It includes the following sections:

- [Section 1.1, "What Is Oracle Fusion Middleware?"](#)
- [Section 1.2, "Oracle Fusion Middleware Components"](#)

For definitions of unfamiliar terms found in this and other books, see the Glossary.

1.1 What Is Oracle Fusion Middleware?

Oracle Fusion Middleware is a collection of standards-based software products that spans a range of tools and services: from Java EE and developer tools, to integration services, identity management, business intelligence, and collaboration. Oracle Fusion Middleware offers complete support for development, deployment, and management.

For information about Oracle Fusion Middleware concepts, see *Understanding Oracle Fusion Middleware*.

1.2 Oracle Fusion Middleware Components

Oracle Fusion Middleware provides the following components:

- Oracle WebLogic Server, an enterprise-ready Java application server that supports the deployment of mission-critical applications in a robust, secure, highly available, and scalable environment. Oracle WebLogic Server is an ideal foundation for building applications based on service-oriented architecture (SOA).

See Also: *Understanding Oracle WebLogic Server*

- Oracle SOA Suite, a complete set of service infrastructure components, in a service-oriented architecture, for designing, deploying, and managing composite applications. Oracle SOA Suite enables services to be created, managed, and orchestrated into composite applications and business processes. Composites enable you to easily assemble multiple technology components into one SOA composite application.

See Also: *Administering Oracle SOA Suite and Oracle Business Process Management Suite*

- Oracle HTTP Server, which provides a Web listener for Java EE applications and the framework for hosting static and dynamic pages and applications over the Web. Based on the proven technology of the Apache HTTP Server, Oracle HTTP Server includes significant enhancements that facilitate load balancing, administration, and configuration.

See Also: *Administering Oracle HTTP Server*

- Oracle Web Services Manager, which provides a way to centrally define and manage policies that govern Web services operations, including access control (authentication and authorization), reliable messaging, Message Transmission Optimization Mechanism (MTOM), WS-Addressing, and Web services management. Policies can be attached to multiple Web services, requiring no modification to the existing Web services.

See Also: *Administering Web Services*

- Oracle Platform Security, which provides enterprise product development teams, systems integrators, and independent software vendors (ISVs) with a standards-based, portable, integrated, enterprise-grade security framework for Java Standard Edition (Java SE) and Java Enterprise Edition (Java EE) applications.

Oracle Platform Security provides an abstraction layer in the form of standards-based application programming interfaces (APIs) that insulate developers from security and identity management implementation details. With Oracle Platform Security, developers do not need to know the details of cryptographic key management or interfaces with user repositories and other identity management infrastructures. When you use Oracle Platform Security, in-house developed applications, third-party applications, and integrated applications benefit from the same uniform security, identity management, and audit services across the enterprise.

See Also: *Securing Applications with Oracle Platform Security Services*

- Oracle Data Integrator provides a fully unified solution for building, deploying, and managing complex data warehouses or as part of data-centric architectures in a SOA or business intelligence environment. In addition, it combines all the elements of data integration — data movement, data synchronization, data quality, data management, and data services—to ensure that information is timely, accurate, and consistent across complex systems.

See Also: *Administering Oracle Data Integrator*

Part II

Basic Administration

This part describes basic administration tasks for Oracle Fusion Middleware.

Part II contains the following chapters:

- [Chapter 2, "Getting Started Managing Oracle Fusion Middleware"](#)
- [Chapter 3, "Wiring Components to Work Together"](#)
- [Chapter 4, "Starting and Stopping Oracle Fusion Middleware"](#)
- [Chapter 5, "Managing Ports"](#)

Getting Started Managing Oracle Fusion Middleware

When you install Oracle Fusion Middleware, you install the binary files, such as executable files, jar files, and libraries. Then, you use configuration tools to configure the software. This chapter provides information you need to get started managing Oracle Fusion Middleware, including information about the tools you use.

This chapter includes the following sections:

- [Section 2.1, "Overview of Oracle Fusion Middleware Administration Tools"](#)
- [Section 2.2, "Getting Started Using Oracle Enterprise Manager Fusion Middleware Control"](#)
- [Section 2.3, "Getting Started Using Oracle WebLogic Server Administration Console"](#)
- [Section 2.4, "Getting Started Using the Oracle WebLogic Scripting Tool \(WLST\)"](#)
- [Section 2.5, "Getting Started Using the Fusion Middleware Control MBean Browsers"](#)
- [Section 2.6, "Changing the Administrative User Password"](#)
- [Section 2.7, "Configuring Node Manager"](#)
- [Section 2.8, "Basic Tasks for Configuring and Managing Oracle Fusion Middleware"](#)

2.1 Overview of Oracle Fusion Middleware Administration Tools

After you install and configure Oracle Fusion Middleware, you can use the graphical user interfaces or command-line tools to manage your environment.

Oracle offers the following primary tools for managing your Oracle Fusion Middleware installations:

- Oracle Enterprise Manager Fusion Middleware Control. See [Section 2.2](#).
- Oracle WebLogic Server Administration Console. See [Section 2.3](#)
- The Oracle Fusion Middleware command-line tools. See [Section 2.4](#).
- The Fusion Middleware Control MBean Browser. See [Section 2.5](#).

Note that you should use these tools, rather than directly editing configuration files, to perform all administrative tasks unless a specific procedure requires you to edit a file. Editing a file may cause the settings to be inconsistent and generate problems.

Both Fusion Middleware Control and Oracle WebLogic Server Administration Console are graphical user interfaces that you can use to monitor and administer your Oracle Fusion Middleware environment. You can install Fusion Middleware Control and the Administration Console when you install most Oracle Fusion Middleware components.

Note the following:

- If you install a standalone Oracle WebLogic Server, Fusion Middleware Control is not installed. Only the Administration Console is installed.
- If you install Oracle JDeveloper, neither Fusion Middleware Control or the Administration Console are installed. They can be installed if you install Oracle Fusion Middleware Application Developer.

You can perform some tasks with either tool, but for other tasks, you can only use one of the tools. [Table 2–1](#) lists some common tasks and the recommended tool.

Table 2–1 Comparing Fusion Middleware Control and WebLogic Server Administration Console

Task	Tool to Use
Manage Oracle WebLogic Server	Use:
Create additional Managed Servers	Fusion Middleware Control
Clone Managed Servers	WebLogic Server Administration Console
Cluster Managed Servers	Fusion Middleware Control
Start and stop Oracle WebLogic Server	Fusion Middleware Control or WebLogic Server Administration Console
Add users and groups	WebLogic Server Administration Console if using the default embedded LDAP; if using another LDAP server, use the LDAP server's tool
Manage Data Sources	Use:
Create data sources	Fusion Middleware Control or WebLogic Server Administration Console
Create connection pools	Fusion Middleware Control or WebLogic Server Administration Console
Manage JMS Resources	Use:
Create JMS queues	WebLogic Server Administration Console
Configure advanced queuing	WebLogic Server Administration Console
Manage SOA environment	Use:
Deploy SOA Composite applications	Fusion Middleware Control
Monitor SOA Composite applications	Fusion Middleware Control
Modify Oracle BPEL Process Manager MBean properties	Fusion Middleware Control
Debug applications such as Oracle BPEL Process Manager applications	Fusion Middleware Control
ADF Applications	Use:
Deploy ADF applications	Fusion Middleware Control
Java EE applications	Use:

Table 2–1 (Cont.) Comparing Fusion Middleware Control and WebLogic Server Administration Console

Task	Tool to Use
Deploy Java EE applications	WebLogic Server Administration Console or Fusion Middleware Control
Security	Use:
Configure and manage auditing	Fusion Middleware Control
Configure SSL	WebLogic Server Administration Console for Oracle WebLogic Server Fusion Middleware Control for Java components and system components. See Chapter 6 .
Change passwords	WebLogic Server Administration Console
Manage Components	Use:
View and manage log files	Fusion Middleware Control for most log files WebLogic Server Administration Console for the following logs: <i>DOMAIN_HOME/servers/server_name/logs/access.log</i> <i>DOMAIN_HOME/servers/server_name/data/ldap/log/EmbeddedLDAP.log</i> <i>DOMAIN_HOME/servers/server_name/data/ldap/log/EmbeddedLDAPAccess.log</i>
Change ports	WebLogic Server Administration Console for Oracle WebLogic Server and Java components For some system components, Fusion Middleware Control. See the administration guide for the component.
Manage Oracle HTTP Server	Fusion Middleware Control
Start and stop components	Fusion Middleware Control
Start and stop applications	Fusion Middleware Control

2.2 Getting Started Using Oracle Enterprise Manager Fusion Middleware Control

Fusion Middleware Control is a Web browser-based, graphical user interface that you can use to monitor and administer your domain. It can manage an Oracle WebLogic Server domain with its Administration Server, one or more Managed Servers, clusters, the Oracle Fusion Middleware components that are installed, configured, and running in the domain, and the applications you deploy.

Fusion Middleware Control organizes a wide variety of performance data and administrative functions into distinct, Web-based home pages for the domain, servers, components, and applications. The Fusion Middleware Control home pages make it easy to locate the most important monitoring data and the most commonly used administrative functions—all from your Web browser.

The following topics are discussed in this section:

- [Displaying Fusion Middleware Control](#)
- [Using Fusion Middleware Control Help](#)
- [Navigating Within Fusion Middleware Control](#)

- [Understanding Users and Roles for Fusion Middleware Control](#)
- [Viewing and Managing the WebLogic Domain](#)
- [Viewing and Managing Components](#)

2.2.1 Displaying Fusion Middleware Control

To display Fusion Middleware Control, you enter the Fusion Middleware Control URL, which includes the name of the host and the administration port number assigned during the installation. The following shows the format of the URL:

```
http://hostname.domain:port/em
```

The port number is the port number of the Administration Server. By default, the port number is 7001. The port number is listed in the following file:

```
DOMAIN_HOME/config/config.xml
```

For some installation types, such as Web Tier, if you saved the installation information by clicking Save on the last installation screen, the URL for Fusion Middleware Control is included in the file that is written to disk (by default to your home directory). For other installation types, the information is displayed on the Create Domain screen of the Configuration Wizard when the configuration completes.

To display Fusion Middleware Control:

1. Enter the URL in your Web browser. For example:

```
http://host1.example.com:7001/em
```

2. Enter the Oracle Fusion Middleware administrator user name and password and click **Login**.

2.2.2 Using Fusion Middleware Control Help

At any time while using the Fusion Middleware Control Console, you can select **Help** from the *username* menu at the top of the page to get more information. From the Help menu, you can select the following:

- **Contents**, which lists the contents of Help.
- **Help for This Page**, which provides context-sensitive help for the current page.
- **How Do I?**, which links to tutorial information in the documentation.
- **Documentation Library**, which links to the library on the Oracle Technology Network.
- **User Forums**, which links to Discussion Forums on the Oracle Technology Network.
- **Oracle Technology Network**, which links to the Oracle Technology Network.

2.2.3 Navigating Within Fusion Middleware Control

Fusion Middleware Control displays the target navigation pane on the left and the content pane on the right. For example, when you first log in to Fusion Middleware Control, the domain home page is displayed on the right.

From the target navigation pane, you can expand the tree and select an Oracle WebLogic Server domain, an Oracle WebLogic Server Managed Server, a component, an application, or a Metadata Repository.

When you select a target, such as a Managed Server or a component, the target's home page is displayed in the content pane and that target's menu is displayed at the top of the page, in the context pane. For example, if you select a Managed Server, the WebLogic Server menu is displayed. You can also view the menu for a target by right-clicking the target in the navigation pane.

The following figure shows the target navigation pane and the home page of an Managed Server. Because a Managed Server was selected, the dynamic target menu listed in the context pane is the WebLogic Server menu.

The screenshot shows the Oracle Enterprise Manager Fusion Middleware Control interface. The interface is divided into several panes:

- Target Navigation Pane:** Contains a tree view of targets. A right-click context menu is open over the 'soa_server1' target, showing options like 'Home', 'Administration', and 'Target Information'.
- Content Pane:** Displays the home page for the selected target, 'soa_server1'. It includes a 'Summary' section with details like 'Up Since', 'Version', 'State', 'Health', 'Server Type', 'Cluster', 'CPU Usage', 'Heap Usage', 'Java Vendor', and 'Java Version'. It also has a 'Tools' section with a link to the 'WebLogic Server Administration Console'.
- Context Pane:** Located at the top right, it shows the user is logged in as 'weblogic' and provides a 'Refresh Icon'.
- Change Center:** Located at the top left, it shows 'Changes' and options to 'Start Up' or 'Shut Down...'.
- Response and Load Graph:** A line graph showing 'Request Processing Time (ms)' and 'Requests (per minute)' over time.

Annotations in the image point to various UI elements:

- Dynamic Target Menu:** Points to the menu items above the 'soa_server1' target.
- Context Pane:** Points to the top right area showing the user and refresh icon.
- Change Center:** Points to the top left area with 'Changes' and control buttons.
- Expand All Collapse All:** Points to the 'View' dropdown in the Target Navigation Pane.
- Right-Click Target Menu:** Points to the context menu over the 'soa_server1' target.

In the preceding figure, the following items are called out:

- **WebLogic Domain Menu** provides a list of operations that you can perform on the domain. The WebLogic Domain menu is always available.
- **Change Center** shows the changes made and allows you to lock and edit the configuration, release the configuration, activate changes, undo all changes, and change preferences. It also allows you to start and stop recording your session, and view the recording.
- **Target Navigation Pane** lists all of the targets in the domain in a navigation tree.
- **Content Pane** shows the current page for the target. When you first select a target, that target's home page is displayed.
- **Dynamic Target Menu** provides a list of operations that you can perform on the currently selected target. The menu that is displayed depends on the target you select. The menu for a specific target contains the same operations as those in the **Right-Click Target Menu**.
- **Right-Click Target Menu** provides a list of operations that you can perform on the currently selected target. The menu is displayed when you right-click the target

name in the target navigation pane. In the figure, even though the WebLogic Server is selected and its home page is displayed, the right-click target menu displays the operations for a metadata repository because the user has right-clicked the metadata repository.

The menu for a specific target contains the same operations as those in the **Dynamic Target Menu**.

- **Target Name** is the name of the currently selected target.
- **Target Information Icon** provides information about the target. For example, for a domain, it displays the target name, the version, and the domain home.
- **Context Pane** provides the name of the target, the name of the current user, the host name, and the time of the last page refresh, as well as the Refresh icon.
- **View** lets you expand or collapse the navigation tree.
- The *username* menu provides links to Help, Accessibility, information about Fusion Middleware Control, and logging out.
- **Refresh** indicates when the page is being refreshed. Click it to refresh a page with new data. (Refreshing the browser window refreshes the page but does not retrieve new data.)

In addition, from the home pages of targets such as the Administration Server or Managed Servers, you can access the WebLogic Server Administration Console.

[Table 2–2](#) describes some common ways you can navigate within Fusion Middleware Control.

Table 2–2 Navigating Within Fusion Middleware Control

To:	Take This Action:
View all of the targets in the domain	From the View menu, select Expand All .
Operate on the domain	Select the WebLogic Domain menu, which is always available at the top left of Fusion Middleware Control.
Operate on a target	Right-click the target in the target navigation pane . The target menu is displayed. Alternatively, you can select the target and use the dynamic target menu in the context pane.
Return to the target's home page	Click the target name at the top left-hand corner of the context pane .
Refresh a page with new data	Click the Refresh icon in the top right of the context pane .
Return to a previous page	Click the breadcrumbs, which appear below the context pane. The breadcrumbs appear when you drill down in a target. For example, choose Logs from the WebLogic Server menu, then View Log Messages. Select a log file and click View Log File. The breadcrumbs show: Log Messages > Log Files > View Log File: <i>logfile_name</i>
View the host on which the target is running	Select the target in the target navigation pane and view the host name in the target's context pane . You can also view the host name by clicking the Target Information icon.
View a server log file	Right-click the server name in the target navigation pane . Choose Logs , and then View Log Messages to see a summary of log messages and to search log files.

2.2.4 Understanding Users and Roles for Fusion Middleware Control

To access Fusion Middleware Control and perform tasks, you must have the appropriate role. Fusion Middleware Control uses the Oracle WebLogic Server security realm and the roles defined in that realm. If a user is not granted one of these roles, the user cannot access Fusion Middleware Control.

Each role defines the type of access a user has, as described in [Table 2-3](#).

Table 2-3 Roles Supported by Fusion Middleware Control

Role	Actions Allowed
Administrator	All access. An administrator has full privileges, including creating and deleting instances and modifying the configuration.
Deployer	Deploy, undeploy, and redeploy applications, modify the configuration of applications, start and stop applications, create and delete JDBC and JMS resources, and modify JDBC and JMS resources, as well as all of the privileges of the Monitor role.
Operator	Start and stop servers and applications, and all of the privileges of the Monitor role.
Monitor	View configuration, status of servers and applications, metrics, log files and log messages.

[Table 2-4](#) summarizes the privileges of each role that is supported by Fusion Middleware Control.

Table 2-4 Privileges for the Supported Roles

Privileges	Administrator	Deployer	Operator	Monitor
Edit session operations: start or release session, activate or undo changes	Yes	Yes	No	No
Server, Cluster, Template, or Machine				
Lifecycle operations: create, delete	Yes	No	No	No
Modify configuration	Yes	No	No	No
Control operations: start, stop, resume	Yes	No	Yes	No
View configuration	Yes	Yes	Yes	Yes
Application Deployments				
Lifecycle operations: deploy, undeploy, redeploy	Yes	Yes	No	No
Modify configuration	Yes	Yes	No	No
Control operations: start, stop	Yes	Yes	Yes	No
JDBC and JMS resources				
Lifecycle operations: create, delete	Yes	Yes	No	No
Modify configuration	Yes	Yes	No	No
Control operations: start, stop	Yes	No	No	No
View configuration	Yes	Yes	Yes	Yes

Table 2-4 (Cont.) Privileges for the Supported Roles

Privileges	Administrator	Deployer	Operator	Monitor
Startup and Shutdown Classes, Coherence Clusters				
Lifecycle operations: create, delete	Yes	No	No	No
Modify configuration	Yes	Yes	No	No
View configuration	Yes	Yes	Yes	Yes

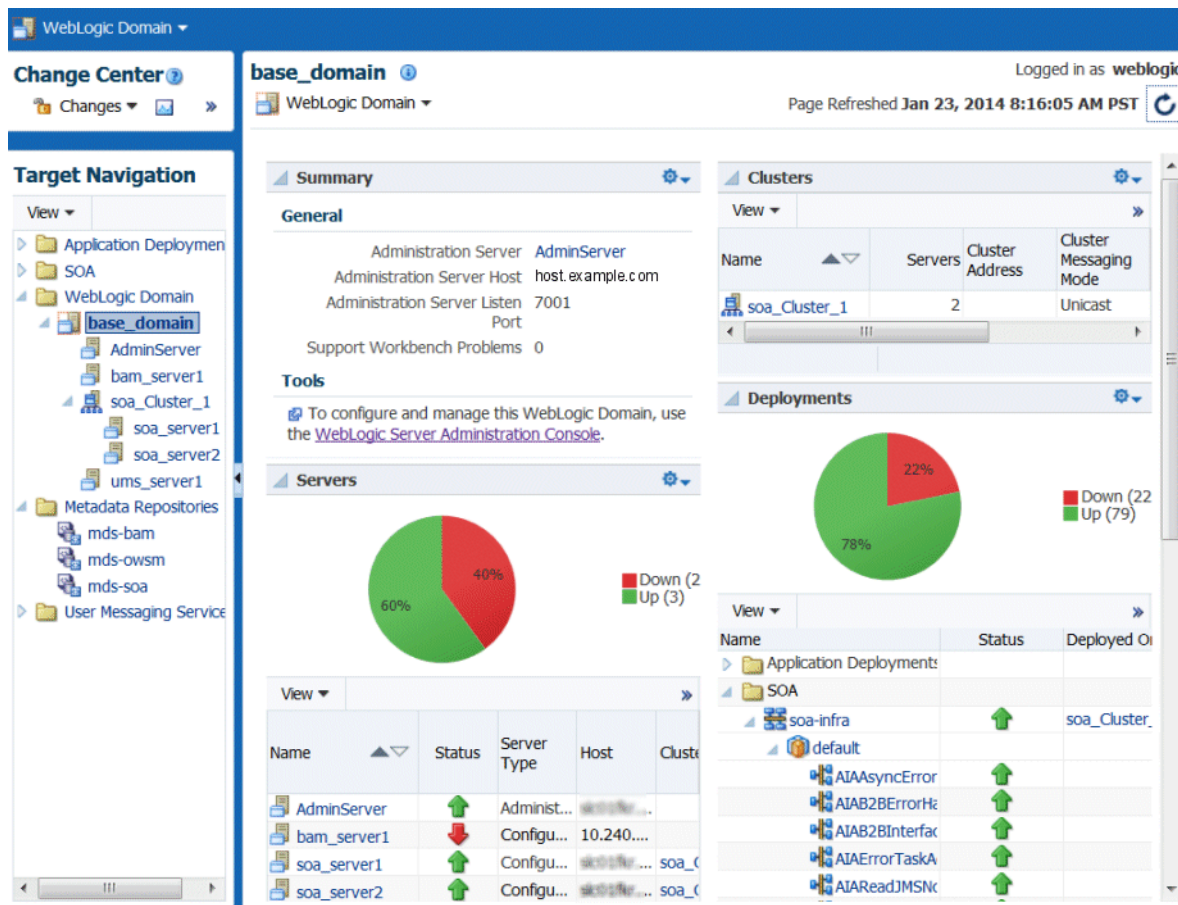
Note that the information in Table 2-4 is based on the default out-of-the-box security policy for WebLogic Resources and MBeans. You can manage the default security policies in the Administration Console, as described in "Use roles and policies to secure resources" in the *Oracle WebLogic Server Administration Console Online Help*.

For more information, see "Understanding WebLogic Resource Security" in *Securing Resources Using Roles and Policies for Oracle WebLogic Server*.

2.2.5 Viewing and Managing the WebLogic Domain

When you log in to Fusion Middleware Control, the first page you see is the domain home page. You can also view this page at any time by selecting Home in the WebLogic Domain menu.

The following figure shows the domain home page:



The WebLogic Domain menu is displayed at the top of the page. From this menu, you can monitor and configure the domain.

The WebLogic Domain menu is always displayed, even if you have selected other entities.

You can view the routing topology by selecting **Routing Topology** from the WebLogic Domain menu. The Topology Viewer provides you with a high-level view of the topology, including Managed Servers, deployed applications, and the routing configuration. See [Section 11.3](#) for information about using the Topology Viewer.

2.2.6 Viewing and Managing Components

From the target navigation pane, you can drill down to view and manage the components in your domain.

For example, to view and manage Oracle SOA Suite, take the following steps:

1. In the target navigation pane, expand **SOA**.
2. Select the SOA instance.

The home page for the SOA instance is displayed, as shown in the following figure:

The screenshot shows the Oracle Enterprise Manager Fusion Middleware Control interface for an SOA instance. The top navigation bar includes 'soa-infra' and 'SOA Infrastructure'. The main content area is divided into several sections:

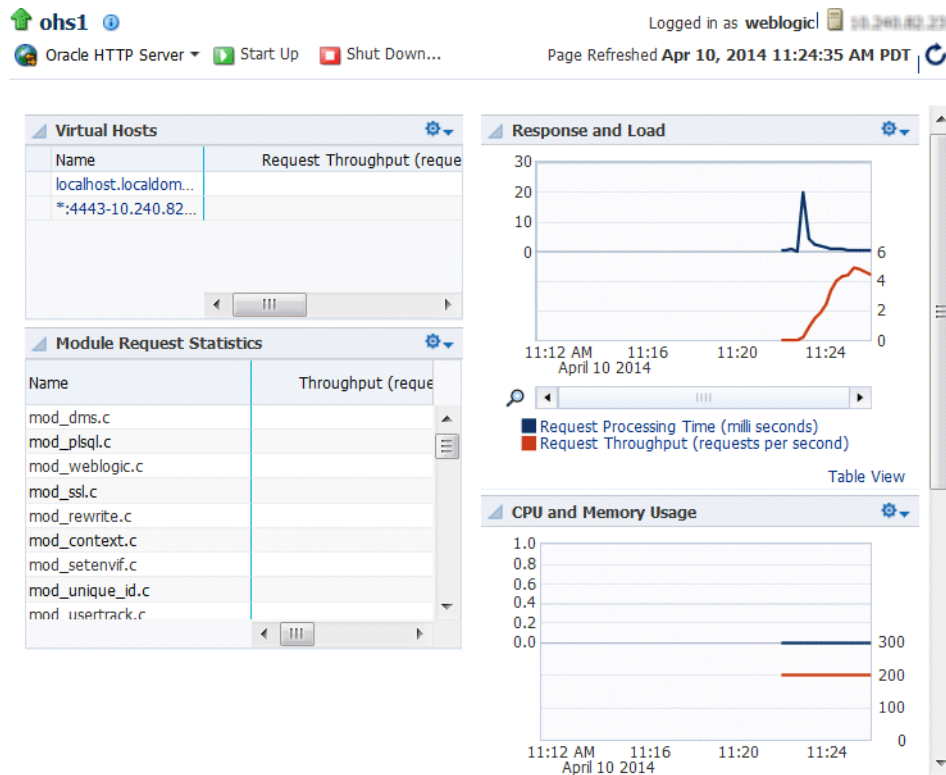
- Key Configuration:** Profile: SOA FOUNDATION WITH B2B, Instance Tracking: Production, Default Query Duration: Last 24 Hours, Auto Purge: Enabled.
- Business Transaction Faults:** Last* 24 Hours, Refresh region to show the latest data. Click graph to...
- SOA Runtime Health:** soa_cluster_1 Initialized Successfully, soa-infra (soa_server2), soa-infra (soa_server1), soa-infra (ess_server1).
- Composites and Adapters Availability:** soa_server1, No Composite Start-Up Errors, No EIS Connectivity Errors, All Composites are UP, All adapter service endpoints are UP.

3. From the SOA Infrastructure menu, you can perform many administrative tasks, such as starting, stopping, and monitoring Oracle SOA Suite and deploying SOA composite applications.

You can also view and manage system components. For example, to view and manage Oracle HTTP Server, take the following steps:

1. From the navigation pane, expand **HTTP_Server**.
2. Select the Oracle HTTP Server instance, for example, ohs1.

The home page for the Oracle HTTP Server ohs1 is displayed, as shown in the following figure:



- From the HTTP Server menu, you can perform many administrative tasks, such as starting, stopping, and monitoring Oracle HTTP Server.

For more information about monitoring components, see [Section 11.1.5](#).

2.3 Getting Started Using Oracle WebLogic Server Administration Console

Oracle WebLogic Server Administration Console is a Web browser-based, graphical user interface that you use to manage an Oracle WebLogic Server domain. It is accessible from any supported Web browser with network access to the Administration Server.

Use the Administration Console to:

- Configure, start, and stop WebLogic Server instances
- Configure WebLogic Server clusters
- Configure WebLogic Server services, such as database connectivity (JDBC) and messaging (JMS)
- Configure security parameters, including creating and managing users, groups, and roles
- Configure and deploy Java EE applications
- Monitor server and application performance
- View server and domain log files

- View application deployment descriptors
- Edit selected run-time application deployment descriptor elements

2.3.1 Displaying the Oracle WebLogic Server Administration Console

To display the Administration Console:

1. Enter the following URL in a browser:

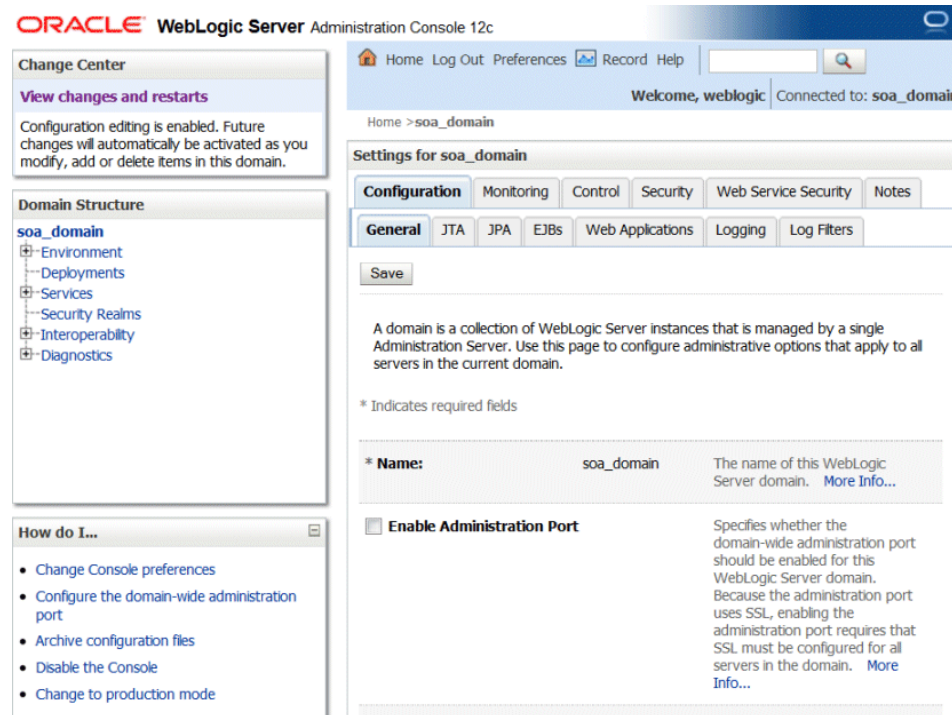
```
http://hostname:port_number/console
```

The port number is the port number of the Administration Server. By default, the port number is 7001.

The login page is displayed.

2. Log in using the user name and password supplied during installation or another administrative user that you created.

Oracle WebLogic Server Administration Console is displayed as shown in the following figure:



Alternatively, you can access the Administration Console from Fusion Middleware Control, from the home pages of targets such as the Administration Server or Managed Servers.

2.3.2 Locking the WebLogic Server Configuration

Before you make configuration changes, lock the domain configuration, so you can make changes to the configuration while preventing other accounts from making changes during your edit session. To lock the domain configuration:

1. Locate the Change Center in the upper left of the Administration Console screen.

2. From the Changes menu, select **Lock & Edit** to lock the configuration edit hierarchy for the domain.

As you make configuration changes using the Administration Console, you click **Save** (or in some cases **Finish**) on the appropriate pages. This does not cause the changes to take effect immediately. The changes take effect when you click **Activate Changes** in the Change Center. At that point, the configuration changes are distributed to each of the servers in the domain. If the changes are acceptable to each of the servers, then they take effect. If any server cannot accept a change, then all of the changes are rolled back from all of the servers in the domain. The changes are left in a pending state; you can then either edit the pending changes to resolve the problem or revert to the previous configuration.

You can also lock the configuration by using the WLST command, `startEdit`:

```
startEdit()
```

For more information about the `startEdit` command and the `stopEdit` command, which releases locks, see "startEdit" and "stopEdit" in the *WLST Command Reference for WebLogic Server*.

2.4 Getting Started Using the Oracle WebLogic Scripting Tool (WLST)

The Oracle WebLogic Scripting Tool (WLST) is a command-line scripting environment that you can use to create, manage, and monitor Oracle WebLogic Server domains. It is based on the Java scripting interpreter, Jython. In addition to supporting standard Jython features such as local variables, conditional variables, and flow-control statements, WLST provides a set of scripting functions (commands) that are specific to WebLogic Server. You can extend the WebLogic scripting language to suit your needs by following the Jython language syntax.

The following topics describe using WLST to manage Oracle Fusion Middleware components:

- [Using WLST with Java Components](#)
- [Using Custom WLST Commands](#)
- [Using WLST Commands with System Components](#)

2.4.1 Using WLST with Java Components

You can use WLST commands with Java components. You can use them in the following ways:

- Interactively, on the command line
- In script mode, supplied in a file
- Embedded in Java code

For example, to invoke WLST interactively, and connect to the WebLogic Server, use the following commands:

```
WL_HOME/server/bin/setWLSEnv.sh
WL_HOME/common/bin/wlst.sh
connect('username', 'password', 'localhost:7001')
```

To display information about WLST commands and variables, enter the `help` command. For example, to display a list of categories for online commands, enter the following:

```
wls:/base_domain/serverConfig> help('online')
help('activate')      Activate the changes.
help('addListener')   Add a JMX listener to the specified MBean.
help('adminHome')     Administration MBeanHome.
help('cancelEdit')    Cancel an edit session.
help('cd')             Navigate the hierarchy of beans.
help('cmo')           Current Management Object.
.
.
.
```

To monitor the status, you use the WLST `state` command, using the following format:

```
state(name, type)
```

For example to get the status of the Managed Server `wls_server1`, use the following command:

```
wls:/WLS_domain/serverConfig> state('wls_server1', 'Server')
Current state of 'wls_server1' : RUNNING
```

For more information about WLST, see the *WLST Command Reference for WebLogic Server*.

2.4.2 Using Custom WLST Commands

Many components, such as Oracle SOA Suite, Oracle Platform Security Services (OPSS), Oracle Fusion Middleware Audit Framework, and MDS, and services such as SSL and logging, provide custom WLST commands.

To use those custom commands, you must invoke the WLST script from the Oracle Common home. Do not use the WLST script in the WebLogic Server home.

For the following services, as well as components such as Oracle ADF and Oracle SOA Suite, invoke WLST from the Oracle Common home:

- Oracle Metadata Services
- Diagnostic Framework
- Dynamic Monitoring Service (DMS)
- Logging
- Oracle Platform Security Services
- Secure Sockets Layer (SSL)
- Oracle JRF
- Oracle Web Services
- Oracle Web Services Manager

The script is located at:

```
(UNIX) ORACLE_HOME/oracle_common/common/bin/wlst.sh
(Windows) ORACLE_HOME\oracle_common\common\bin\wlst.cmd
```

2.4.3 Using WLST Commands with System Components

You can use WLST commands with **system components**. The following component is a system component:

- Oracle HTTP Server

For system components, you can only use the WLST commands listed in [Table 2–5](#). See *WLST Command Reference for WebLogic Server* for information about whether a command can be invoked in online or offline mode.

Table 2–5 WLST Commands for System Components

WLST Command	Description	For more information:
create	Creates an instance of the system component with defaults.	The create command in <i>WLST Command Reference for WebLogic Server</i>
displayLogs	Displays the messages in a log file.	The displayLogs command in <i>WLST Command Reference for Infrastructure Components</i> and Section 12.3.1.2
displayMetricTableNames	Displays the names of the DMS metric tables.	The displayMetricTableNames command in <i>WLST Command Reference for Infrastructure Components</i>
displayMetricTables	Displays the contents of the DMS metric tables.	The displayMetricTables command in <i>WLST Command Reference for Infrastructure Components</i>
dumpMetrics	Displays the available DMS metrics.	The dumpMetrics command in <i>WLST Command Reference for Infrastructure Components</i>
listLogs	Lists the log files.	The listLogs command in <i>WLST Command Reference for Infrastructure Components</i> and Section 12.3.1.2
nmKill	Shuts down an instance.	The nmkill command in <i>WLST Command Reference for WebLogic Server</i> and Section 4.3.2.2
nmServerStatus	Returns the status on an instance.	The nmServerStatus command in <i>WLST Command Reference for WebLogic Server</i>
nmStart	Starts an instance.	The nmStart command in <i>WLST Command Reference for WebLogic Server</i> and Section 4.3.2.2
shutdown	Stops a system component instance.	The shutdown command in <i>WLST Command Reference for WebLogic Server</i> and Section 4.3.2.2
start	Starts a system component instance.	The start command in <i>WLST Command Reference for WebLogic Server</i> and Section 4.3.2.2
state	Returns the state of a system component instance.	The state command in <i>WLST Command Reference for WebLogic Server</i> and Section 2.4

To use these commands, you must invoke the WLST script from the Oracle common home in which the component has been installed. Do not use the WLST script in the WebLogic Server home. The script is located at:

```
(UNIX) ORACLE_HOME/oracle_common/common/bin/wlst.sh
```

```
(Windows) ORACLE_HOME\oracle_common\common\bin\wlst.cmd
```

To monitor the status of a system component, you use the WLST `state` command, using the following format:

```
state(component_name, SystemComponent)
```

In online mode, you can use the `cmo` variable to invoke MBean operations that provide even more functionality. For more information about the `cmo` variable, see "Changing the Current Management Object" in *Understanding the WebLogic Scripting Tool*.

To use WLST commands that are specific to a system component, invoke the WLST script from the following location:

```
ORACLE_HOME/component_type/common/bin
```

2.5 Getting Started Using the Fusion Middleware Control MBean Browsers

A **managed bean** (MBean) is a Java object that represents a JMX manageable resource in a distributed environment, such as an application, a service, a component or a device.

The following topics describe MBeans and how to view or configure MBeans:

- [Understanding MBeans](#)
- [Using the System MBean Browser](#)
- [Using the MBeans for a Selected Application](#)

2.5.1 Understanding MBeans

MBeans are defined in the Java EE Management Specification (JSR-77), which is part of Java Management Extensions, or JMX, a set of specifications that allow standard interfaces to be created for managing applications in a Java EE environment. For information about JSR-77, see:

<http://www.oracle.com/technetwork/java/javasee/overview-137048.html>

You can create MBeans for deployment with an application into Oracle WebLogic Server, enabling the application or its components to be managed and monitored through Fusion Middleware Control.

Fusion Middleware Control provides a set of MBean browsers that allow you to browse the MBeans for an Oracle WebLogic Server or for a selected application. You can also perform specific monitoring and configuration tasks from the MBean browser.

The MBeans are organized into three groups: Configuration MBeans, Runtime MBeans, and Application-Defined MBeans.

For more information about MBeans, see "Understanding WebLogic Server MBeans" in *Developing Custom Management Utilities Using JMX for Oracle WebLogic Server*.

2.5.2 Using the System MBean Browser

You can view the System MBean Browser for many entities, including an Oracle WebLogic Server domain, an Administration Server, a Managed Server, or an application. You can search for an MBean, filter the list of MBeans, and refresh the list of MBeans in the MBean navigation tree.

To view the System MBean Browser specific to a particular Oracle WebLogic Server Managed Server and to configure and use the MBeans:

1. From the target navigation pane, expand the domain.
2. Select the Managed Server.
3. From the WebLogic Server menu, choose **System MBean Browser**.
The System MBean Browser page is displayed.
4. Expand a node in the MBean navigation tree and drill down to the MBean you want to access. Select an MBean instance.

If you do not know the location of an MBean, you can search for the MBean:

- a. Click the Find icon at the top of the MBean navigation tree.
 - b. For **Find**, select **MBean Name**.
You can also select Attributes, Operations, or JMX syntax.
 - c. Enter the name of the MBean and click the arrow.
5. To view the MBean's attributes, select the Attributes tab. Some attributes allow you to change their values. To do so, enter the value in the **Value** column.
 6. To view the available operations, select the Operations tab. To perform an operation, click the operation. The Operations page appears. Enter any applicable values and click **Invoke**.

For more information, see the Fusion Middleware Control online help.

2.5.3 Using the MBeans for a Selected Application

You can view, configure, and use the MBeans for a specific application by taking the steps described in [Section 2.5.2](#), and drilling down to the application. As an alternative, you can navigate to an application's MBeans using the following steps:

1. From the target navigation pane, expand **Application Deployments**.
2. Select the application.
3. From the Application Deployments menu, choose **System MBean Browser**.
The System MBean Browser page is displayed, along with the MBean information for the application.
4. To view the MBean's attributes, select the Attributes tab. Some attributes allow you to change their values. To do so, enter the value in the **Value** column.
5. To view the available operations, select the Operations tab. To perform an operation, click the operation. The Operations page appears. Enter any applicable values and click **Invoke**.

2.6 Changing the Administrative User Password

During the Oracle Fusion Middleware installation, you must specify a password for the administration account. Then, you can use this account to log in to Fusion Middleware Control and the Oracle WebLogic Server Administration Console for the first time. You can create additional administrative accounts using the WLST command line or the Oracle WebLogic Server Administration Console.

You can change the password of the administrative user using the command line or the Oracle WebLogic Server Administration Console, as described in the following topics:

- [Changing the Administrative User Password Using the Command Line](#)
- [Changing the Administrative User Password Using the Administration Console](#)

For more information about users, roles, and changing passwords, see "Understanding Users and Roles" in the *Securing Applications with Oracle Platform Security Services*.

2.6.1 Changing the Administrative User Password Using the Command Line

To change the administrative user password or other user passwords using the command line, you invoke the `UserPasswordEditorMBean.changeUserPassword` method, which is extended by the security realm's `AuthenticationProvider` MBean.

For more information, see the `changeUserPassword` method in the *MBean Reference for Oracle WebLogic Server*.

2.6.2 Changing the Administrative User Password Using the Administration Console

To change the password of an administrative user using the Oracle WebLogic Server Administration Console:

1. Navigate to the Oracle WebLogic Server Administration Console. (For example, from the home page of the domain in Fusion Middleware Control, select **To configure and managed this WebLogic Domain, use the Oracle WebLogic Server Administration Console.**)
2. From the Domain Structure pane, select **Security Realms**.
The Summary of Security Realms page is displayed.
3. Select a realm, such as **myrealm**.
The Settings for the realm page is displayed.
4. Select the Users and Groups tab, then the Users tab. Select the user.
The Settings for *user* page is displayed.
5. Select the Passwords tab.
6. Enter the new password, then enter it again to confirm it.
7. Click **Save**.

2.7 Configuring Node Manager

Node Manager allows you to perform common operations, such as starting and stopping, for a Managed Server using the Administration Console or Fusion Middleware Control.

This section describes the following topics:

- [Configuring Node Manager to Start Managed Servers](#)
- [Configuring Node Manager to Use the OPSS Keystore Service](#)

2.7.1 Configuring Node Manager to Start Managed Servers

If a Managed Server contains other Oracle Fusion Middleware products, such as Oracle JRF or Oracle SOA Suite, the Managed Servers environment must be configured to set the correct classpath and parameters. By default, Node Manager is configured when you install Oracle Fusion Middleware.

However, if you do not select automatic configuration, you must provide this environment information through the start scripts, such as `startWebLogic` and `setDomainEnv`, which are located in the following directory:

```
DOMAIN_HOME/bin
```

If the Managed Servers are started by Node Manager (as is the case when the servers are started by the Oracle WebLogic Server Administration Console or Fusion Middleware Control), Node Manager must be instructed to use these start scripts so that the server environments are correctly configured. Specifically, Node Manager must be started with the property `StartScriptEnabled=true`.

There are several ways to ensure that Node Manager starts with this property enabled. As a convenience, Oracle Fusion Middleware provides the following script, which adds the property `StartScriptEnabled=true` to the `nodemanager.properties` file:

```
(UNIX) ORACLE_HOME/oracle_common/common/bin/setNMProps.sh.  
(Windows) ORACLE_HOME\oracle_common\common\bin\setNMProps.cmd
```

For example, on Linux, execute the `setNMProps` script and start Node Manager:

```
ORACLE_HOME/oracle_common/common/bin/setNMProps.sh  
DOMAIN_HOME/bin/startNodeManager.sh
```

When you start Node Manager, it reads the `nodemanager.properties` file with the `StartScriptEnabled=true` property, and uses the start scripts when it subsequently starts Managed Servers. Note that you need to run the `setNMProps` script only once.

Also note that when the `StartScriptEnable` property is set to true, the Node Manager reads the `startWebLogic` script, which in turns reads the `setDomainEnv` script. As a result, you must make any tuning changes by editing the `setDomainEnv` script. Any changes that are performed using the command line or Administration Console will not be implemented when Node Manager starts the servers. For example, if you use the Administration Console to change the server start arguments, those changes are written to `config.xml`, but the Node Manager ignores these settings and uses those in `setDomainEnv`.

See "Using Node Manager" in the *Administering Node Manager for Oracle WebLogic Server* for other methods of configuring and starting Node Manager.

2.7.2 Configuring Node Manager to Use the OPSS Keystore Service

If you created a domain that included Oracle JRF and you configured Node Manager as "per domain", you can configure Node Manager to use the Oracle Platform Security Services Keystore Service. Take the following steps:

1. Configure the Keystore Service, as described in "Keystore Management with the Keystore Service" in *Securing Applications with Oracle Platform Security Services*.
2. Configure Node Manager by editing the following file:

```
DOMAIN_HOME/nodemanager/nodemanager.properties
```

In the file, specify the following properties:


```

KeyStores=CustomIdentityAndDemoTrust
CustomIdentityKeyStoreType=KSS
CustomIdentityKeyStoreFileName=kss://system/keystore_name
CustomIdentityKeyStorePassPhrase= keystore_passphrase
CustomIdentityAlias= key store alias
CustomIdentityPrivateKeyPassPhrase= keystore_private_key_passphrase

```

Oracle Platform Security Services Keystore Service is not supported for a "per host" Node Manager. In certain circumstances, however, a "per host" Node Manager will attempt to load the keystore service. To prevent that, you must specify `UseKSSForDemo=false` in the following file:

```
ORACLE_HOME/oracle_common/common/nodemanager/nodemanager.properties
```

Note: Oracle Platform Security Services adds the following arguments to the `startNodeManager` script, which triggers the use of the Keystore Service instead of a JKS -based keystore:

```

-Doracle.security.jps.config=DOMAIN_
HOME/config/fmwconfig/jps-config-jse.xml
-Dcommon.components.home=MW_HOME/oracle_common
-Dopss.version=12.1.3

```

If you configure Node Manager to start WebLogic Server without the `startWebLogic` script (`StartScriptEnabled=false`), you must add these arguments to the server's `ServerStartMBean Arguments` field using an administration tool, such as WLST or the Administration console.

In addition, you must add the following to the CLASSPATH definition:

```
MW_HOME/oracle_common/modules/oracle.jps_12.1.3/jps-manifest.jar.
```

2.8 Basic Tasks for Configuring and Managing Oracle Fusion Middleware

The following provides a summary of the steps you need to take to configure and manage a basic Oracle Fusion Middleware environment after you have installed the software:

1. Configure Oracle WebLogic Server and components, such as Oracle SOA Suite or Oracle HTTP Server. See *Planning an Installation of Oracle Fusion Middleware*.
2. Configure Node Manager. See [Section 2.7](#).
3. Configure SSL. See [Chapter 6](#).
4. Create and manage metadata repositories, including the MDS Repository. See [Section 14.2](#).
5. Deploy an application. See [Chapter 10](#).
6. Configure load balancing. You can configure load balancing between different components or applications. See the *High Availability Guide*.
7. Back up your environment. See [Chapter 16](#).
8. Monitor your environment and manage log files. See [Chapter 11](#) and [Chapter 12](#).
9. Expand your environment. See [Chapter 19](#).

This guide also describes other tasks that you may need to perform, depending on your Oracle Fusion Middleware environment.

Note: The procedures in this book for the most part assume that you are using the standard installation topology, which consists of a domain that contains an Administration Server and a cluster containing two Managed Servers.

For more information about the standard topology, see "Understanding the Oracle Fusion Middleware Infrastructure Standard Installation Topology" in *Installing and Configuring the Oracle Fusion Middleware Infrastructure*.

Wiring Components to Work Together

This chapter describes service tables and how to wire particular Oracle Fusion Middleware components together.

It contains the following sections:

- [Section 3.1, "Understanding Service Tables"](#)
- [Section 3.2, "Viewing Service Tables"](#)
- [Section 3.3, "Wiring Components Together"](#)

3.1 Understanding Service Tables

A **service table** provides a way for service providers to publish endpoint information about their services, and clients of these services to query and bind to these services. A service table is a single table in a database schema. There is one row for every endpoint that is published to it. The service table schema is initially created by the Repository Creation Utility.

See "Understanding the Service Table Schema" in *Creating Schemas with the Repository Creation Utility* for information about the service table schema.

The local service table is associated with a domain. It contains endpoints that are offered by that domain. For the local service table, the data source name is LocalSvcTblDataSource.

For example, by default, the service table contains endpoint information for Oracle Web Services Manager and Fusion Middleware Control.

3.2 Viewing Service Tables

You can view the service tables using Fusion Middleware Control:

1. From the WebLogic Domain menu, choose **Cross Component Wiring**, then **Service Tables**.

The Service Tables page is displayed.

soa_domain ⓘ Logged in as **weblogic**

WebLogic Domain ▼ Page Refreshed **Mar 14, 2014 12:30:14 PM PDT** ↻

/Domain_soa_domain/soa_domain > Service Tables

Service Tables

This page lists the contents of Local Service. You can add, edit and delete EndPoints from this page. To view the contents of the Share Local Service and to enable sharing / unsharing of End Points, configure the Shared Service Table Data Source.

Local Service

JDBC Data Source

Name LocalSvcTblDataSource
 URL jdbc:oracle:thin:@//host.example.com:1521/ORCL.US.ORACLE.COM
 State Running

View ▼ + Add 🔍 View ✎ Edit... ✕ Delete...

Service Type	Service ID	Connection
fmw.soa:t3	urn:oracle:fmw.soa:t3	t3://10.240.82.231:7006,10.240.82.231:7006,10.240.82.
mod_weblogic	urn:oracle:fmw.soa.infra.mod_weblogic	t3://10.240.82.231:7005,10.240.82.231:7006,10.240.82.
mod_weblogic	urn:oracle:fmw.soa.composer.mod_we...	t3://10.240.82.231:7005,10.240.82.231:7006,10.240.82.
mod_weblogic	urn:oracle:fmw.worklistapp.mod_weblo...	t3://10.240.82.231:7005,10.240.82.231:7006,10.240.82.

2. You can view, edit, or delete the properties of an endpoint by clicking one of the buttons.

3.3 Wiring Components Together

When you install and configure Oracle Fusion Middleware, most of the cross-component wiring is automatically performed. However, there may be cases when you want to connect another component or to change the current wiring. For example:

- To connect Oracle HTTP Server to the Administration Server, so that it is connected to Fusion Middleware Control and the Administration Console. See [Section 3.3.1](#).
- To connect Oracle HTTP Server to an Oracle WebLogic Server cluster or server, so that applications can be routed through Oracle HTTP Server to the cluster or server. See [Section 3.3.2](#).
- To connect the Oracle Web Services Manager agent to the Policy Manager. See "Using Cross-Component Wiring for Auto-Discovery of Policy Manager" in *Securing Web Services and Managing Policies with Oracle Web Services Manager*.

3.3.1 Wiring Oracle HTTP Server to the Administration Server

You can connect Oracle HTTP Server to the Administration Server so that you can access Fusion Middleware Control and the Administration Console through the Oracle HTTP Server, as described in the following topics:

- [Why Wire Oracle HTTP Server to the Administration Server?](#)
- [Connecting Oracle HTTP Server to the Administration Server](#)

3.3.1.1 Why Wire Oracle HTTP Server to the Administration Server?

By default, you can access Fusion Middleware Control and the WebLogic Server Administration Console by directly accessing the Administration Server and the default Administration port (7001). For example:

```
http://hostname:7001/em
```

However, in many cases, only the Oracle HTTP Server instances in the Web tier are exposed to the Internet as part of a DMZ, and the application tier (where the

Administration Server resides) is protected by an additional firewall. In those cases, you can configure the Oracle HTTP Server instances in the Web tier to route any requests to the management consoles to the Administration Server. This allows administrators to access the management consoles from outside the firewall using the standard front-end URL, which is used to access the Oracle HTTP Server instances. Configuring the Web server in this way can also serve as a way of verifying the configuration of your domain, in preparation for deploying applications. When you deploy applications to the application tier, you can then configure Oracle HTTP Server in a similar manner so your application users can access the applications through the front-end HTTP Server instance URL

For a more complete example of how you might configure Oracle HTTP Server as part of a Web tier, see "Configuring Oracle HTTP Server for High Availability" the *High Availability Guide*.

3.3.1.2 Connecting Oracle HTTP Server to the Administration Server

To connect Oracle HTTP Server to the Administration Server:

1. From the navigation pane, expand **HTTP Server**.
2. Select an Oracle HTTP Server instance, such as ohs1.

The Oracle HTTP Server page is displayed.

3. From the Oracle HTTP Server menu, select **Administration**, then **mod_wl_ohs Configuration**.

The mod_wl_ohs Configuration page is displayed, as shown in the following figure:

The screenshot shows the Oracle HTTP Server Administration console for instance 'ohs1'. The user is logged in as 'weblogic1'. The navigation pane shows 'Oracle HTTP Server' expanded, with 'Start Up' and 'Shut Down...' options. The main content area displays the 'mod_wl_ohs Configuration' page. At the top, there is an 'Information' section stating that all changes require a server restart. Below this is the 'mod_wl_ohs Configuration' section with 'Apply' and 'Revert' buttons. The 'General' section contains the following fields: 'WebLogic Cluster' (text input), 'WebLogic Host' (text input), 'WebLogic Port' (text input), a 'Dynamic Server List ON' checkbox, 'Error Page' (text input), 'WebLogic Temp Directory' (text input), and 'Exclude Path or Mime Type' (text input). The 'Match Expressions' section has 'Add Row' and 'Remove' buttons, and a table with one row containing 'Expression' and 'No data to display'.

4. To connect to the Administration Server:
 - For **WebLogic Host**, enter the host name for the Administration Server.

- For **WebLogic Port**, enter the server port for the Administration Server.
Alternatively, you can click the search icon. Then, select the Administration Server and click **OK**. The fields will be filled in automatically.
5. In the Locations section, click **AutoFill**.
All valid WebLogic Server endpoint locations are displayed.
 6. From the table, select `/em`.
 7. To add the Administration Console:
 - a. Click **Add Row**.
 - b. For location, enter `/console`.
 - c. For **WebLogic Host**, enter the host name for the Administration Server.
 - d. For **Port**, enter the Administration Server port number.
 8. Click **Apply**.
 9. Shutdown the Oracle HTTP Server instance, then start it again.

3.3.2 Routing Applications Through Oracle HTTP Server to Oracle WebLogic Server

To connect Oracle HTTP Server so that requests are routed through Oracle HTTP Server to Oracle WebLogic Server:

1. From the navigation pane, expand the domain, then **HTTP Server**.
2. Select an Oracle HTTP Server instance, such as `ohs1`.
The Oracle HTTP Server page is displayed.
3. From the Oracle HTTP Server menu, select **Administration**, then **mod_wl_ohs configuration**.
The `mod_wl_ohs` Configuration page is displayed.
4. To have requests routed to the cluster, for **WebLogic Cluster**, enter the cluster address. Alternatively, you can click the search Icon and select the cluster. The fields will be filled automatically.
To have requests routed to a single WebLogic server:
 - For **WebLogic Host**, enter the server name.
 - For **WebLogic Port**, enter the server port.Alternatively, you can click the search icon next to **WebLogic Host**. Then, select the server from the list and click **OK**. The fields will be filled in automatically.
Note that if you enter values for both WebLogic Cluster and WebLogic Host and Port. WebLogic Cluster will be used.
5. In the Locations section, click **AutoFill**.
All valid WebLogic Server endpoint locations are displayed.
6. Select the application from the table.
7. Click **Apply**.
8. Shutdown the Oracle HTTP Server instance, then start it again.

Starting and Stopping Oracle Fusion Middleware

This chapter describes procedures for starting and stopping Oracle Fusion Middleware, including the Administration Server, Managed Servers, and components.

It contains the following sections:

- [Section 4.1, "Overview of Starting and Stopping Procedures"](#)
- [Section 4.2, "Starting and Stopping Oracle WebLogic Server Administration and Managed Servers"](#)
- [Section 4.3, "Starting and Stopping Components"](#)
- [Section 4.4, "Starting and Stopping Fusion Middleware Control"](#)
- [Section 4.5, "Starting and Stopping Applications"](#)
- [Section 4.6, "Starting and Stopping Your Oracle Fusion Middleware Environment"](#)
- [Section 4.7, "Starting and Stopping: Special Topics"](#)

4.1 Overview of Starting and Stopping Procedures

Oracle Fusion Middleware is a flexible product that you can start and stop in different ways, depending on your requirements. In most situations, you can use Fusion Middleware Control, Oracle WebLogic Server Administration Console, or the WLST commands to start or stop Oracle Fusion Middleware components.

These tools are completely compatible and, in most cases, can be used interchangeably. For example, you can start a J2EE component using WLST and stop it using Fusion Middleware Control.

4.2 Starting and Stopping Oracle WebLogic Server Administration and Managed Servers

You can start Oracle WebLogic Server Administration Servers using the WLST command line. You can start and stop Managed Servers using scripts, the WLST command line, the WebLogic Server Administration Console, or Fusion Middleware Control. The following sections describe how to start and stop WebLogic Servers using the WLST command line, Fusion Middleware Control, or both:

- [Starting and Stopping Administration Server](#)
- [Starting and Stopping Node Manager](#)
- [Starting and Stopping Managed Servers](#)

- [Enabling Servers to Start Without Supplying Credentials](#)
- [Setting Up Oracle WebLogic Server as a Windows Service](#)

4.2.1 Starting and Stopping Administration Server

You can start and stop the Oracle WebLogic Server Administration Server using the WLST command line or a script. When you start or stop the Administration Server, you also start or stop the processes running in the Administration Server, including the WebLogic Server Administration Console and Fusion Middleware Control.

For example, to start an Administration Server, use the following script:

```
DOMAIN_HOME/bin/startWebLogic.sh
```

To stop an Administration Server, use the following script:

```
DOMAIN_HOME/bin/stopWebLogic.sh
  username password [admin_url]
```

4.2.2 Starting and Stopping Node Manager

By default, Node Manager is configured when you configure Oracle Fusion Middleware. If Node Manager is not configured, it is very important to change the Node Manager property `StartScriptEnabled` to `True`. If this property is set to `False`, you will encounter errors or problems when starting Managed Servers configured for use by Oracle Fusion Middleware components. See [Section 2.7.1](#) for more information.

You can start Node Manager using the WLST command line or a script.

For example, to start Node Manager, use the following script:

```
(UNIX) DOMAIN_HOME/bin/startNodeManager.sh
(Windows) DOMAIN_HOME\bin\startNodeManager.cmd
```

To stop Node Manager, close the command shell in which it is running.

Alternatively, after having set the `nodemanager.properties` attribute `QuitEnabled` to `true` (the default is `false`), you can use WLST to connect to Node Manager and shut it down. For more information, see `stopNodeManager` in the *WLST Command Reference for WebLogic Server*.

4.2.3 Starting and Stopping Managed Servers

You can start and stop Managed Servers using Fusion Middleware Control or WLST commands and scripts, as described in the following topics:

- [Starting and Stopping Managed Servers Using Fusion Middleware Control](#)
- [Starting and Stopping Managed Servers Using Scripts](#)

4.2.3.1 Starting and Stopping Managed Servers Using Fusion Middleware Control

Fusion Middleware Control and the Oracle WebLogic Server Administration Console use Node Manager to start Managed Servers. If you are starting a Managed Server that does not contain Oracle Fusion Middleware products other than Oracle WebLogic Server, you can start the servers using the procedure in this section.

However, if the Managed Server contains other Oracle Fusion Middleware products, such as Oracle JRF or Oracle SOA Suite, you must first configure Node Manager, as described in [Section 2.7.1](#).

To start or stop a WebLogic Server Managed Server using Fusion Middleware Control:

1. From the navigation pane, expand the domain.
2. Select the Managed Server.
3. From the WebLogic Server menu, choose **Control**, then **Start Up** or **Shut Down**.

Alternatively, you can right-click the server, then choose **Control**, then **Start Up** or **Shut Down**.

4.2.3.2 Starting and Stopping Managed Servers Using Scripts

You can use a script or WLST to start and stop a WebLogic Server Managed Server.

For example, to start a WebLogic Server Managed Server, use the following script:

```
(UNIX) DOMAIN_HOME/bin/startManagedWebLogic.sh
      managed_server_name admin_url
(Windows) DOMAIN_HOME\bin\startManagedWebLogic.cmd
      managed_server_name admin_url
```

When prompted, enter your user name and password.

To stop a WebLogic Server Managed Server, use the following script:

```
(UNIX) DOMAIN_HOME/bin/stopManagedWebLogic.sh
      managed_server_name admin_url
(Windows) DOMAIN_HOME\bin\stopManagedWebLogic.cmd
      managed_server_name admin_url
```

When prompted, enter your user name and password.

For information about using WLST to start and stop Managed Servers, see "Managing the Server Life Cycle" in *Understanding the WebLogic Scripting Tool*.

4.2.4 Enabling Servers to Start Without Supplying Credentials

You can enable the Administration Server and Managed Servers to start without prompting you for the administrator user name and password.

1. For the Administration Server, create a boot.properties file:
 - a. Create the following directory:


```
DOMAIN_HOME/servers/AdminServer/security
```
 - b. Use a text editor to create a file called boot.properties in the security directory created in the previous step, and enter the following lines in the file:

```
username=adminuser
password=password
```

2. For each Managed Server:
 - a. Create the following directory:


```
DOMAIN_HOME/servers/server_name/security
```
 - b. Copy the boot.properties file you created for the Administration Server to the security directory you created in the previous step.
3. Restart the Administration Server and Managed Servers, as described in [Section 4.2.1](#) and [Section 4.2.3](#).

Note: When you start the Administration Server or Managed Server, the user name and password entries in the file are encrypted.

For security reasons, minimize the time the entries in the file are left unencrypted. After you edit the file, start the server as soon as possible in order for the entries to be encrypted.

For more information, see "Boot Identity Files" in *Administering Server Startup and Shutdown for Oracle WebLogic Server*.

4.2.5 Setting Up Oracle WebLogic Server as a Windows Service

If you want a WebLogic Server instance to start automatically when you boot a Windows host computer, you can set up the server as a Windows service. For complete information, see "Setting Up a WebLogic Server Instance as a Windows Service" in *Administering Server Startup and Shutdown for Oracle WebLogic Server*.

However, that chapter describes the process for a standalone Oracle WebLogic Server installation. When Oracle WebLogic Server is part of an Oracle Fusion Middleware environment, you must set the environment to include references to `ORACLE_COMMON`. To do that, the script that you create is slightly different from that in "Example Script for Setting Up a Managed Server as a Windows Service". The following shows the correct script:

```
echo off
SETLOCAL
set DOMAIN_NAME=myWLSdomain
set USERDOMAIN_HOME=d:\Oracle\config\domains\myWLSdomain
set SERVER_NAME=myWLSserver
set PRODUCTION_MODE=true
set
JAVA_OPTIONS=-Dweblogic.Stdout="d:\Oracle\config\domains\myWLSdomain\
stdout.txt" -Dweblogic.Stderr="d:\Oracle\config\domains\myWLSdomain\stderr.txt"
set ADMIN_URL=http://adminserver:7501
set MEM_ARGS=-Xms40m -Xmx250m
call %USERDOMAIN_HOME%\bin\setDomainEnv.cmd
call "d:\Oracle_home\wlserver\server\bin\installSvc.cmd"
ENDLOCAL
```

4.3 Starting and Stopping Components

You can start and stop components using the command line, the WebLogic Server Administration Console, or Fusion Middleware Control, depending upon the component. The following topics describe how to start and stop components using Fusion Middleware Control and the command line:

- [Starting and Stopping Components Using Fusion Middleware Control](#)
- [Starting and Stopping Components Using the Command Line](#)

4.3.1 Starting and Stopping Components Using Fusion Middleware Control

To start or stop a component:

1. From the navigation pane, navigate to the component.
2. Select the component, such as **OHS**.
3. From the dynamic target menu, choose **Control**, then **Start Up** or **Shut Down**.

4.3.2 Starting and Stopping Components Using the Command Line

If a component is a Java component, you can use WLST commands to start and stop the component. If a component is a system component, you can use scripts to call WLST commands to start and stop the components, as described in the following topics:

- [Starting and Stopping Java Components](#)
- [Starting and Stopping System Components](#)

4.3.2.1 Starting and Stopping Java Components

To start and stop Java components, use the WLST `startApplication` and `stopApplication` commands:

```
startApplication(appName, [options])
stopApplication(appName, [options])
```

For example, to start Oracle Web Services Manager Policy Manager, use the following command:

```
startApplication("wsm-pm")
```

4.3.2.2 Starting and Stopping System Components

If a component is a system component, you can use scripts to call WLST commands to start and stop the components or you can use WLST commands:

- To start and stop system components using scripts, use the `startComponent` and `stopComponent` scripts. You can use this method for system components, such as Oracle HTTP Server, in a standalone domain or a WebLogic Server domain. You must invoke them from the host that contains the Administration Server.

The scripts are located in

```
(UNIX) DOMAIN_HOME/bin
(Windows) DOMAIN_HOME\bin
```

To start or stop a component using these scripts, use the following syntax:

```
./startComponent.sh component_name [storeUserConfig] [showErrorStack]
./stopComponent.sh component_name [storeUserConfig] [showErrorStack]
```

In the syntax:

- *component_name*: The name of the component instance, such as ohs1.
- *storeUserConfig*: When specified, the script will prompt you for the user name and password. Then, it will ask you if you want to store the user configuration in a properties file. If you specify *y*, it creates a user configuration file and an associated key file. The user configuration file contains an encrypted user name and password. The key file contains a secret key that is used to encrypt and decrypt the user name and password. The following shows the names and location of the properties files:

```
user_home/.wlst/nm-key-domain_name.props
user_home/.wlst/nm-cfg-domain_name.props
```

After you have stored the information in the properties file, when you run the scripts subsequently, you will not be prompted for a user name and password.

- `showErrorStack`: Provides more detailed error information, including all of the messages in the error stack. Specify this option if you need to determine the cause of errors.

For example, to start an Oracle HTTP Server instance called `ohs1`:

```
./startComponent.sh ohs1
```

You can also use these scripts to start and stop system components remotely. In that case, the scripts read the configuration to determine the location of the component.

- To start system components using WLST commands, you can use one of the following methods:
 - The `nmstart` command. You can use this method for Oracle HTTP Server in a standalone domain or a WebLogic Server domain.

For example, to start the Oracle HTTP Server component OHS1, use the following WLST commands:

```
nmConnect(domainName='domain_name', username='username',
password='password')
nmstart(serverName='OHS1', serverType='OHS')
```

- The WLST start command. You can use this method for Oracle HTTP Server in a standalone domain.

For example, to start the Oracle HTTP Server component OHS1, use the following WLST commands:

```
connect('username', 'password', 'hostname:port')
start('OHS1')
```

- To stop system components using WLST commands, use the WLST `nmkill` command.

For example, to kill the Oracle HTTP Server component OHS1, use the following WLST commands:

```
nmKill(serverName='ohs1', serverType='OHS')
```

To decide which method to use, note the following:

- If you are using a WLST script, use the WLST commands.
- To quickly start and stop system components interactively, use the scripts.
- To start and stop system components remotely, use the scripts.

4.4 Starting and Stopping Fusion Middleware Control

If Fusion Middleware Control is configured for a domain, it is automatically started or stopped when you start or stop an Oracle WebLogic Server Administration Server, as described in [Section 4.2.1](#).

4.5 Starting and Stopping Applications

You can start and stop applications using Fusion Middleware Control, the WebLogic Server Administration Console, or the WLST command line. The following topics describe how to start and stop applications using Fusion Middleware Control and the command line:

- [Starting and Stopping Java EE Applications Using Fusion Middleware Control](#)
- [Starting and Stopping Java EE Applications Using WLST](#)

4.5.1 Starting and Stopping Java EE Applications Using Fusion Middleware Control

To start or stop a Java EE application using Fusion Middleware Control:

1. From the navigation pane, expand **Application Deployments**.
2. Select the application.
3. From the Application Deployment menu, choose **Control**, then **Start Up** or **Shut Down**.

To start or stop a SOA Composite application using Fusion Middleware Control:

1. From the navigation pane, expand the domain, then **SOA**, and then **soa-infra**.
2. Select the application.
3. On the SOA Composite page, click **Start Up** or **Shut Down**.

4.5.2 Starting and Stopping Java EE Applications Using WLST

To start or stop a Java EE application with the WLST command line, use the following commands:

```
startApplication(appName, [options])
stopApplication(appName, [options])
```

The application must be fully configured and available in the domain. The `startApplication` command returns a `WLSTProgress` object that you can access to check the status of the command. In the event of an error, the command returns a `WLSTException`. For more information about the `WLSTProgress` object, see "WLSTProgress Object" in *Understanding the WebLogic Scripting Tool*.

4.6 Starting and Stopping Your Oracle Fusion Middleware Environment

This section provides procedures for starting and stopping an Oracle Fusion Middleware environment. An environment can consist of an Oracle WebLogic Server domain, an Administration Server, multiple Managed Servers, Java components, system components, including Identity Management components, and a database used as a repository for metadata. The components may be dependent on each other. Therefore, it is important to start and stop them in a particular order.

4.6.1 Starting an Oracle Fusion Middleware Environment

To start an Oracle Fusion Middleware environment:

1. Start the database that hosts the metadata schemas. The following steps illustrate one method for starting the database.
 - a. Navigate to the location of the database. For example, the database may reside on a different host than Oracle Fusion Middleware.
 - b. Set the `ORACLE_HOME` environment variable to the Oracle home for the database.
 - c. Set the `ORACLE_SID` environment variable to the SID for the database (default is `orcl`.)

- d. Start the Net Listener:

```
ORACLE_HOME/bin/lsnrctl start
```

- e. Start the database instance:

```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> startup
SQL> quit
```

For more information about starting an Oracle Database, see the *Oracle Database Administrator's Guide*.

2. Start the Administration Server as described in [Section 4.2.1](#).
3. Start Node Manager as described in [Section 4.2.2](#).
4. Start any Oracle Identity Management components, such as Oracle Internet Directory, which form part of your environment.
5. Start the Managed Servers as described in [Section 4.2.3.2](#).

Note: The start up of a Managed Server will typically start up the applications which are deployed to it. Therefore, it should not be necessary to manually start applications after the Managed Server startup.

6. Start all other system components, such as Oracle HTTP Server:

```
(UNIX) DOMAIN_HOME/bin/startComponent.sh component_name
(Windows) DOMAIN_HOME\bin\startComponent.cmd component_name
```

4.6.2 Stopping an Oracle Fusion Middleware Environment

To stop an Oracle Fusion Middleware environment:

1. Stop system components, such as Oracle HTTP Server. You can stop them in any order:

```
(UNIX) DOMAIN_HOME/bin/stopComponent.sh component_name
(Windows) DOMAIN_HOME\bin\stopComponent.cmd component_name
```

2. Stop the Managed Servers, as described in [Section 4.2](#). Any applications deployed to the server are also stopped.
3. Stop any 11g Oracle Identity Management components, such as Oracle Internet Directory, which form part of your environment.
4. Stop the Administration Server as described in [Section 4.2.1](#).
5. Stop Node Manager as described in [Section 4.2.2](#).
6. Start the database that hosts the metadata schemas. The following steps illustrate one method for stopping the database:
 - a. Navigate to the location of the database. For example, the database may reside on a different host than Oracle Fusion Middleware.
 - b. Set the ORACLE_HOME environment variable to the Oracle home for the database.
 - c. Set the ORACLE_SID environment variable to the SID for the database (default is orcl).
 - d. Stop the database instance:

```

ORACLE_HOME/bin/sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> shutdown
SQL> quit

```

- e. Stop the Net Listener:

```
ORACLE_HOME/bin/lsnrctl stop
```

For more information about stopping an Oracle Database, see the *Oracle Database Administrator's Guide*.

4.7 Starting and Stopping: Special Topics

This section contains the following special topics about starting and stopping Oracle Fusion Middleware:

- [Starting and Stopping in High Availability Environments](#)
- [Forcing a Shutdown of Oracle Database](#)

4.7.1 Starting and Stopping in High Availability Environments

There are special considerations and procedures for starting and stopping High Availability environments, such as:

- Oracle Fusion Middleware Cold Failover Cluster
- Oracle Application Server Disaster Recovery

See the *High Availability Guide* for information about starting and stopping in high-availability environments.

4.7.2 Forcing a Shutdown of Oracle Database

If you find that the Oracle Database instance is taking a long time to shut down, you can use the following commands to force an immediate shutdown:

```

ORACLE_HOME/bin/sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> SHUTDOWN IMMEDIATE;

```

An immediate database shutdown proceeds with the following conditions:

- No new connections are allowed, nor are new transactions allowed to be started, after the statement is issued.
- Any uncommitted transactions are rolled back. (If long uncommitted transactions exist, this method of shutdown might not complete quickly, despite its name.)
- Oracle does not wait for users currently connected to the database to disconnect. Oracle implicitly rolls back active transactions and disconnects all connected users.

The next startup of the database will not require any instance recovery procedures.

For more information about shutting down an Oracle Database, *Oracle Database Administrator's Guide* in the Oracle Database documentation library

Managing Ports

This chapter describes how to view and change Oracle Fusion Middleware port numbers, such as those used by Oracle WebLogic Server or Oracle HTTP Server.

It contains the following sections:

- [Section 5.1, "About Managing Ports"](#)
- [Section 5.2, "Viewing Port Numbers"](#)
- [Section 5.3, "Changing the Port Numbers Used by Oracle Fusion Middleware"](#)

5.1 About Managing Ports

Many Oracle Fusion Middleware components and services use ports. Most port numbers are assigned during domain creation. As an administrator, it is important to know the port numbers used by these services, and to ensure that the same port number is not used by two services on your host.

For some ports, you can specify a port number assignment during domain creation.

See Also: [Appendix D](#) for a list of port numbers. Refer to the installation guide for directions on overriding port assignments during installation.

5.2 Viewing Port Numbers

You can view the port numbers currently in use with the command line or Fusion Middleware Control, as described in the following topics:

- [Viewing Port Numbers Using the Command Line](#)
- [Viewing Port Numbers Using Fusion Middleware Control](#)

5.2.1 Viewing Port Numbers Using the Command Line

To view the port numbers for Oracle WebLogic Server, you can use the WLST `get` command, with an attribute. For example, to get the Administration Port, use the following command:

```
wls:/WLS_domain/serverConfig> get('AdministrationPort')
9002
```

5.2.2 Viewing Port Numbers Using Fusion Middleware Control

You can view the port numbers of the domain, the Administration Server, Managed Servers, or components, such as Oracle HTTP Server, using Fusion Middleware Control.

For example, to view the ports of a domain:

1. From the WebLogic Domain menu, choose **Monitoring**, then **Port Usage**.

The Port Usage page is displayed, as shown in the following figure:

soa_domain ⓘ Logged in as weblogic
 WebLogic Domain ▼ Page Refreshed Mar 19, 2014 11:58:34 AM PDT ↻

Port Usage

Show All ▼

Port in Use	IP Address	Component	Channel	Protocol
7007	10.240.82.231	soa_server2	Default[ldap]	ldap
7001	10.240.82.231	AdminServer	Default[http]	http
7001	10.240.82.231	AdminServer	Default[iiop]	iiop
7001	10.240.82.231	AdminServer	Default[ldap]	ldap
7006	10.240.82.231	soa_server1	Default[CLUSTER-BR...]	CLUSTER-BROADC...
7006	10.240.82.231	soa_server1	Default[http]	http
7007	10.240.82.231	soa_server2	Default[CLUSTER-BR...]	CLUSTER-BROADC...
7007	10.240.82.231	soa_server2	Default[t3]	t3
7006	10.240.82.231	soa_server1	Default[t3]	t3
7001	10.240.82.231	AdminServer	Default[snmp]	snmp
7007	10.240.82.231	soa_server2	Default[snmp]	snmp
7007	10.240.82.231	soa_server2	Default[http]	http
7006	10.240.82.231	soa_server1	Default[ldap]	ldap
7006	10.240.82.231	soa_server1	Default[iiop]	iiop
7007	10.240.82.231	soa_server2	Default[iiop]	iiop
7001	10.240.82.231	AdminServer	Default[t3]	t3
7006	10.240.82.231	soa_server1	Default[snmp]	snmp

Optionally, you can filter the ports shown by selecting a Managed Server from **Show**.

The Port Usage detail table shows the ports that are in use, the IP Address, the component, the channel, and the protocol.

You can also view similar pages for the Administration Server, Managed Servers, and components, such as Oracle HTTP Server, by navigating to the target and choosing **Port Usage** from the target's menu.

5.3 Changing the Port Numbers Used by Oracle Fusion Middleware

You can change the port numbers for some Oracle Fusion Middleware components, using Fusion Middleware Control, Oracle WebLogic Server Administration Console, or the command line.

Note: You can change a port number to any number you want, if it is an unused port. You do not have to use a port in the allotted port range for the component. See [Appendix D](#) for information on allotted port ranges.

This section provides the following topics:

- [Changing the Oracle WebLogic Server Listen Ports](#)

- [Changing the Oracle HTTP Server Listen Ports](#)
- [Changing the Oracle Database Net Listener Port](#)

For information about changing other ports, see:

- "Configuring Node Manager" in *Administering Node Manager for Oracle WebLogic Server* for information about changing the Node Manager port.

5.3.1 Changing the Oracle WebLogic Server Listen Ports

You can change the non-SSL (HTTP) listen port and the SSL (HTTPS) listen port for an Administration Server or a Managed Server using the Oracle WebLogic Server Administration Console or WLST, as described in the following topics:

- [Changing the Oracle WebLogic Server Listen Ports Using the Administration Console](#)
- [Changing the Oracle WebLogic Server Listen Ports Using WLST](#)

See *Administering Server Environments for Oracle WebLogic Server* for more information about changing Oracle WebLogic Server ports.

5.3.1.1 Changing the Oracle WebLogic Server Listen Ports Using the Administration Console

To change the non-SSL (HTTP) listen port and the SSL (HTTPS) listen port for an Administration Server or a Managed Server using the Oracle WebLogic Server Administration Console:

1. Navigate to the server.
The Settings for *server_name* page is displayed.
2. Select the **Configuration** tab. On the General tab, change the number of the **Listen Port** or **SSL Listen Port**.
3. If the server is running, restart the server.
4. If other components rely on the Oracle WebLogic Server listen ports, you must reconfigure those components.

5.3.1.2 Changing the Oracle WebLogic Server Listen Ports Using WLST

To change the non-SSL (HTTP) listen port and the SSL (HTTPS) listen port for an Administration Server or a Managed Server using the WLST command line. You must run the commands in offline mode; that is, you must not be connected to a server.

For example, to change the Administration Server HTTP listen port to port 8001, use the following WLST commands:

```
readDomain("oracle/config/domains/domain_name")
cd("servers/AdminServer")
cmo.setListenPort(8001)
updateDomain()
```

5.3.2 Changing the Oracle HTTP Server Listen Ports

To change the Oracle HTTP Server Listen ports (non-SSL or SSL), there are often dependencies that must also be set.

The following topics describe how to modify the Oracle HTTP Server HTTP or HTTPS Listen port:

- [Enabling Oracle HTTP Server to Run as Root for Ports Set to Less Than 1024 \(UNIX Only\)](#)
- [Changing the Oracle HTTP Server Non-SSL Listen Port in a WebLogic Server Domain](#)
- [Changing the Oracle HTTP Server SSL Listen Port in a WebLogic Server Domain](#)
- [Changing the Oracle HTTP Server Listen Ports in a Standalone Domain](#)

5.3.2.1 Enabling Oracle HTTP Server to Run as Root for Ports Set to Less Than 1024 (UNIX Only)

By default, Oracle HTTP Server runs as a non-root user (the user that installed Oracle Fusion Middleware). On UNIX systems, if you change the Oracle HTTP Server Listen port number to a value less than 1024, you must enable Oracle HTTP Server to run as root.

For information about enabling the Listen port to run as root see "Starting Oracle HTTP Server Instances on a Privileged Port (Unix Only)" in *Administering Oracle HTTP Server*.

5.3.2.2 Changing the Oracle HTTP Server Non-SSL Listen Port in a WebLogic Server Domain

To change the Oracle HTTP Server non-SSL (HTTP) Listen port, take the following steps. Note that, on a UNIX system, if you are changing the Listen port to a number less than 1024, you must first perform the steps in [Section 5.3.2.1](#).

To change the Oracle HTTP Server Listen port using Fusion Middleware Control:

1. From the navigation pane, expand **HTTP_Server**. Then select the Oracle HTTP Server instance.
2. From the Oracle HTTP Server menu, choose **Administration**, then **Ports Configuration**.
3. Select the Listen port that uses the HTTP protocol, then click **Edit**.
4. Change the port number, then click **OK**.
5. Restart Oracle HTTP Server. (From the Oracle HTTP Server menu, choose **Control**, then **Restart**.)

5.3.2.3 Changing the Oracle HTTP Server SSL Listen Port in a WebLogic Server Domain

To change the Oracle HTTP Server SSL (HTTPS) Listen port, take the following steps. Note that, on a UNIX system, if you are changing the Listen port to a number less than 1024, you must perform the steps in [Section 5.3.2.1](#).

To change the Oracle HTTP Server SSL Listen port using Fusion Middleware Control:

1. From the navigation pane, expand **HTTP_Server**. Then select the Oracle HTTP Server instance.
2. From the Oracle HTTP Server menu, choose **Administration**, then **Ports Configuration**.
3. Select the Listen port that uses the HTTPS protocol, then click **Edit**.
4. Change the port number, then click **OK**.

5. Restart Oracle HTTP Server. (From the Oracle HTTP Server menu, choose **Control**, then **Restart**.)

5.3.2.4 Changing the Oracle HTTP Server Listen Ports in a Standalone Domain

To change the Oracle HTTP Server non-SSL and SSL Listen ports in a standalone domain, modify the following files:

```
DOMAIN_HOME/config/fmwconfig/components/OHS/instances/component_name/httpd.conf
DOMAIN_HOME/config/fmwconfig/components/OHS/instances/component_name/admin.conf
DOMAIN_HOME/config/fmwconfig/components/OHS/instances/component_name/ssl.conf
```

5.3.3 Changing the Oracle Database Net Listener Port

If your environment includes an Oracle Database that functions as a metadata repository, and you want to change the listener port number for that database, perform the procedure in this section.

First, determine if it is necessary to change the listener port number. If you are concerned that you have another database on your host using the same port, both databases can possibly use the same port.

Note that multiple Oracle Database 10g and Oracle Database 11g databases can share the same Oracle Net listener port. If you are using an Oracle Database as a metadata repository on the same host that contains another Oracle Database 10g or Oracle Database 11g database, they can all use port 1521. There is no need to change the listener port number.

Note: To run two listeners that use the same key value on one host, refer to [Section 5.3.3.1, "Changing the KEY Value for an IPC Listener"](#)

The procedure consists of the following tasks:

- [Task 1, "Stop Components"](#)
- [Task 2, "Change the Metadata Repository for Oracle Net Listener Port"](#)
- [Task 3, "Change the System Data Source"](#)

Task 1 Stop Components

Stop all components that use the Metadata Repository. See [Chapter 4](#) for instructions.

Task 2 Change the Metadata Repository for Oracle Net Listener Port

On the metadata repository host:

1. Ensure that the ORACLE_HOME and ORACLE_SID environment variables are set.
2. Stop the metadata repository listener:

```
lsnrctl stop
```

3. Edit the listener.ora file, which is located at:

```
(UNIX) ORACLE_HOME/network/admin/listener.ora
(Windows) ORACLE_HOME\network\admin\listener.ora
```

Under the LISTENER entry, update the value for PORT. Save the file.

4. Edit the `tnsnames.ora` file. The default location is:

```
(UNIX) ORACLE_HOME/network/admin/tnsnames.ora
(Windows) ORACLE_HOME\network\admin\tnsnames.ora
```

Make the following changes to the file:

- a. Update the `PORT` value in each entry that applies to MDS Repository.
- b. Add an entry similar to the following:

```
newnetport =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = tcp) (HOST = hostname) (PORT = port)))
```

In the example, *hostname* is the fully qualified host name and *port* is the new port number.

5. Start the metadata repository listener:

```
lsnrctl start
```

6. Using SQL*Plus, log in to the metadata repository as the SYSTEM user with SYSDBA privileges and run the following command:

```
SQL> ALTER SYSTEM SET local_listener='newnetport' scope=spfile;
```

7. Using SQL*Plus, restart the metadata repository:

```
SQL> SHUTDOWN
SQL> STARTUP
```

Task 3 Change the System Data Source

Change the system data source to use the new port number for the metadata repository. To do so, you can use Fusion Middleware Control:

1. In the Change Center, click **Lock & Edit**.
2. In the navigation pane, expand select the domain.
The WebLogic Domain page is displayed.
3. From the WebLogic Domain menu, select **JDBC Data Sources**.
The Summary of JDBC Data Sources page is displayed.
4. Select the data source you want to change.
The JDBC Data Source page is displayed.
5. Select the Connection Pool tab.
6. To change the database port, modify the **Database URL** field. For example:
`jdbc:oracle:thin:@hostname.domainname.com:1522/orcl`
7. Click **Save**.
8. Restart the servers that use this data source. (Click the Targets tab to see the servers that use this data source.)

5.3.3.1 Changing the KEY Value for an IPC Listener

It is not possible to run two listeners at the same time that are configured to use the same KEY value in their IPC protocol address. By default, the metadata repository listener has its IPC KEY value set to EXTPROC. Hence, if your computer has another

IPC listener that uses the EXTPROC key, you should configure the metadata repository listener to use some other key value such as EXTPROC1.

To change the KEY value of an IPC listener:

1. Stop the listener (ensure that your ORACLE_HOME environment variable is set first):

```
lsnrctl stop
```

2. Edit the listener.ora and tnsnames.ora files. In each file, find the following line:

```
(ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC))
```

Change it to the following:

```
(ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1))
```

3. Restart the listener:

```
lsnrctl start
```


Part III

Secure Communication

This part describes how to secure communications between Oracle Fusion Middleware components. It covers technologies such as Secure Sockets Layer (SSL), keystores, wallets, certificates, and FIPS support.

Part III contains the following chapters:

- [Chapter 6, "Configuring SSL in Oracle Fusion Middleware"](#)
- [Chapter 7, "Managing Keystores, Wallets, and Certificates"](#)
- [Chapter 8, "FIPS 140 Support in Oracle Fusion Middleware"](#)

Configuring SSL in Oracle Fusion Middleware

This chapter provides procedures to secure communications between Oracle Fusion Middleware components in web, middle, and data tiers using Secure Sockets Layer (SSL). It also describes advanced scenarios beyond the basic topologies and explains best practices.

Refer to component-specific documentation to learn about the SSL cipher suite(s) that the client can use during the SSL handshake.

This chapter contains these topics:

- [Section 6.1, "How SSL Works"](#)
- [Section 6.2, "About SSL in Oracle Fusion Middleware"](#)
- [Section 6.3, "Configuring SSL for Configuration Tools"](#)
- [Section 6.4, "Configuring SSL for the Web Tier"](#)
- [Section 6.5, "Configuring SSL for the Middle Tier"](#)
- [Section 6.6, "Configuring SSL for the Data Tier"](#)
- [Section 6.7, "Advanced SSL Scenarios"](#)
- [Section 6.8, "Best Practices for SSL"](#)
- [Section 6.9, "WLST Reference for SSL"](#)

Note: Where SSL connections are configured within Oracle WebLogic Server, this chapter provides references to the relevant Oracle WebLogic Server documentation rather than duplicating the instructions here.

6.1 How SSL Works

This section introduces basic SSL concepts. It contains these topics:

- [What SSL Provides](#)
- [About Private and Public Key Cryptography](#)
- [Keystores and Wallets](#)
- [How SSL Sessions Are Conducted](#)

6.1.1 What SSL Provides

SSL secures communication by providing message encryption, integrity, and authentication. The SSL standard allows the involved components (such as browsers and HTTP servers) to negotiate which encryption, authentication, and integrity mechanisms to use.

- Encryption provides confidentiality by allowing only the intended recipient to read the message. SSL can use different encryption algorithms to encrypt messages. During the SSL handshake that occurs at the start of each SSL session, the client and the server negotiate which algorithm to use. Examples of encryption algorithms supported by SSL include AES, RC4, and 3DES.
- Integrity ensures that a message sent by a client is received intact by the server, untampered. To ensure message integrity, the client hashes the message into a digest using a hash function and sends this message digest to the server. The server also hashes the message into a digest and compares the digests. Because SSL uses hash functions that make it computationally infeasible to produce the same digest from two different messages, the server can tell that if the digests do not match, someone had tampered with the message. An example of a hash function supported by SSL is SHA2.
- Authentication enables the server and client to check that the other party is who it claims to be. When a client initiates an SSL session, the server typically sends its certificate to the client. Certificates are digital identities that are issued by trusted certificate authorities, such as Verisign. [Chapter 7, "Managing Keystores, Wallets, and Certificates"](#) describes certificates in more detail.

The client verifies that the server is authentic and not an imposter by validating the certificate chain in the server certificate. The server certificate is guaranteed by the certificate authority (CA) who signed the server certificate.

The server can also require the client to have a certificate, if the server needs to authenticate the identity of the client.

6.1.2 About Private and Public Key Cryptography

To provide message integrity, authentication, and encryption, SSL uses both private and public key cryptography.

Secret Key Cryptography

Symmetric key cryptography requires a single, secret key shared by two or more parties to secure communication. This key is used to encrypt and decrypt secure messages sent between the parties. It requires prior and secure distribution of the key to each party. The problem with this method is that it is difficult to securely transmit and store the key.

In SSL, each party calculates the secret key individually using random values known to each side. The parties then send encrypted messages using the secret key.

Public Key Cryptography

Public key cryptography solves this problem by employing public and private key pairs and a secure method for key distribution. The freely available public key is used to encrypt messages that can *only* be decrypted by the holder of the associated private key. Together with other security credentials, private key is securely stored in an encrypted container such as an Oracle wallet.

Public key algorithms can guarantee the secrecy of a message. However, they do not necessarily guarantee secure communication because they do not verify the identities

of the communicating parties. To establish secure communication, it is important to verify that the public key used to encrypt a message does in fact belong to the target recipient. Otherwise, a third party can potentially eavesdrop on the communication and intercept public key requests, substituting its own public key for a legitimate key (the man-in-the-middle attack).

To avoid such an attack, it is necessary to verify the owner of the public key with a process called authentication. trusted by both of the communicating parties, a third party known as a certificate authority (CA) can accomplish the authentication process.

The CA issues public key certificates that contain an entity's name, public key, and certain other security credentials. Such credentials typically include the CA name, the CA signature, and the certificate effective dates (From Date, To Date).

The CA uses its private key to encrypt a message, while the public key is used to decrypt it, thus verifying that the message was encrypted by the CA. The CA public key is well known, and does not have to be authenticated each time it is accessed. Such CA public keys are stored in wallets.

6.1.3 Keystores and Wallets

In Oracle Fusion Middleware, components such as Oracle HTTP Server use the Oracle Wallet as their storage mechanism. An Oracle wallet is a container that stores your credentials, such as certificates, trusted certificates, certificate requests, and private keys. You can store Oracle wallets on the file system or in LDAP directories such as Oracle Internet Directory. Oracle wallets can be auto-login or password-protected wallets.

Oracle HTTP Server uses Oracle wallet. Configuring SSL for Oracle HTTP Server thus requires setting up and using Oracle wallets.

Note: As of Oracle Fusion Middleware 12c (12.1.3), you can take advantage of the central storage and unified management available with the Keystore Service to manage wallets and their contents through the export, import, and synchronization features of that service. See the *Infrastructure Security WLST Command Reference* for details about the `importKeyStore`, `exportKeyStore`, and `syncKeyStore` commands.

Other components use a JKS keystore or KSS keystore to store keys and certificates, and configuring SSL for these components requires setting up and using the appropriate keystores.

For more information about configuring keystores and wallets, see:

- [Section 6.2, "About SSL in Oracle Fusion Middleware"](#) for a fuller description of keystore and wallet usage in Oracle Fusion Middleware
- [Chapter 7, "Managing Keystores, Wallets, and Certificates"](#) for a discussion of these terms, and administration details

6.1.4 How SSL Sessions Are Conducted

The SSL protocol has two phases: the handshake phase and the data transfer phase. The handshake phase authenticates the server and optionally the client, and establishes the cryptographic keys that will be used to protect the data to be transmitted in the data transfer phase.

When a client requests an SSL connection to a server, the client and server first exchange messages in the handshake phase. (A common scenario is a browser requesting a page using the `https://` instead of `http://` protocol from a server. The HTTPS protocol indicates the usage of SSL with HTTP.)

Figure 6–1 shows the handshake messages for a typical SSL connection between a Web server and a browser. The following steps are shown in the figure:

1. The client sends a Hello message to the server.
The message includes a list of algorithms supported by the client and a random number that will be used to generate the keys.
2. The server responds by sending a Hello message to the client. This message includes:
 - The algorithm to use. The server selected this from the list sent by the client.
 - A random number, which will be used to generate the keys.
3. The server sends its certificate to the client.
4. The client authenticates the server by checking the validity of the server's certificate, the issuer CA, and optionally, by checking that the host name of the server matches the subject DN. The client sends a Session ID for session caching.
5. The client generates a random value ("pre-master secret"), encrypts it using the server's public key, and sends it to the server.
6. The server uses its private key to decrypt the message to retrieve the pre-master secret.
7. The client and server separately calculate the keys that will be used in the SSL session.

These keys are not sent to each other because the keys are calculated based on the pre-master secret and the random numbers, which are known to each side. The keys include:

- Encryption key that the client uses to encrypt data before sending it to the server
- Encryption key that the server uses to encrypt data before sending it to the client
- Key that the client uses to create a message digest of the data
- Key that the server uses to create a message digest of the data

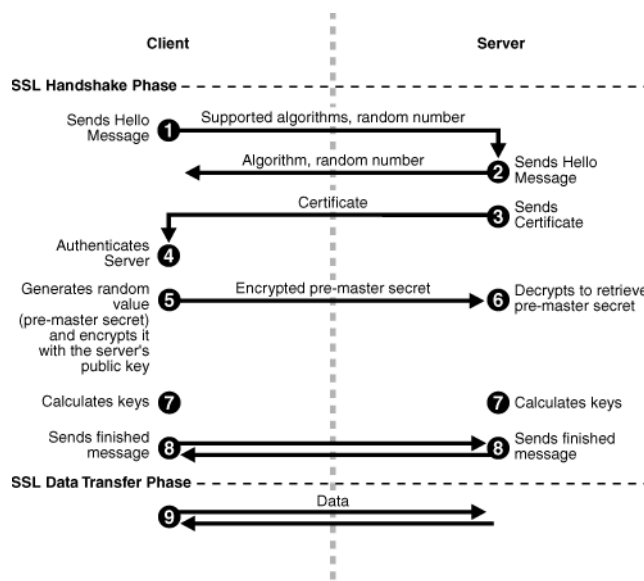
The encryption keys are symmetric, that is, the same key is used to encrypt and decrypt the data.

8. The client and server send a `Finished` message to each other. These are the first messages that are sent using the keys generated in the previous step (the first "secure" messages).

The `Finished` message includes all the previous handshake messages that each side sent. Each side verifies that the previous messages that it received match the messages included in the `Finished` message. This checks that the handshake messages were not tampered with.

9. The client and server now transfer data using the encryption and hashing keys and algorithms.

Figure 6–1 SSL Handshake



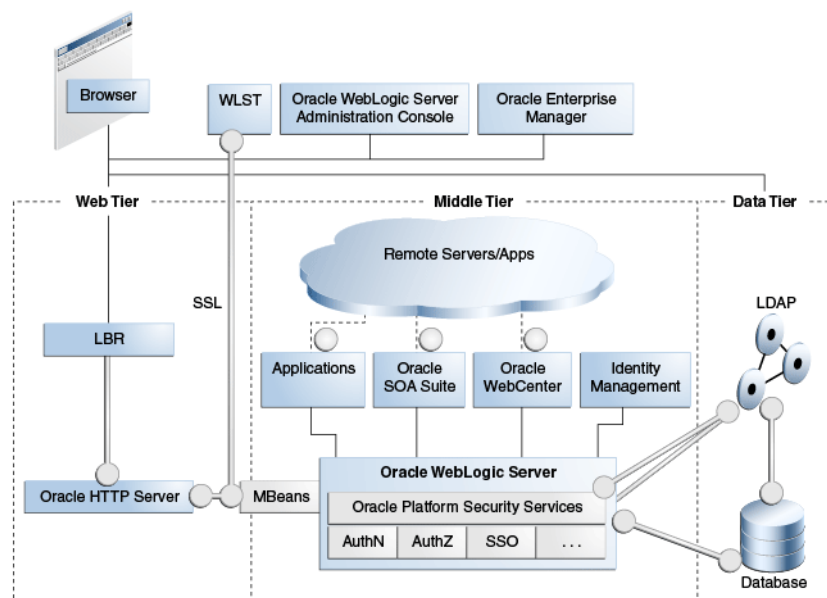
6.2 About SSL in Oracle Fusion Middleware

This section introduces SSL in Oracle Fusion Middleware. It contains these topics:

- [SSL in the Oracle Fusion Middleware Architecture](#)
- [Keystores and Oracle Wallets](#)
- [Authentication Modes](#)
- [Tools for SSL Configuration](#)

6.2.1 SSL in the Oracle Fusion Middleware Architecture

Figure 6–2 SSL in Oracle Fusion Middleware



Notes:

- In [Figure 6–2](#), the label "Oracle Enterprise Manager" refers to the Fusion Middleware Control user interface.
- Other administrative tools are available for specific tasks.

In the Oracle Fusion Middleware architecture shown in [Figure 6–2](#), the circles represent the endpoints that can be SSL-enabled. For configuration details about each endpoint, see:

1. [Section 6.4.2.1, "Enabling SSL for Inbound Requests to Oracle HTTP Server Virtual Hosts Using Fusion Middleware Control"](#) and [Section 6.4.2.2, "Enabling SSL for Inbound Requests to Oracle HTTP Server Virtual Hosts Using WLST"](#)
2. [Section 6.4.2.3, "Enabling SSL for Outbound Requests from Oracle HTTP Server"](#)
3. [Section 6.5.1.1, "Configuring Inbound SSL to Oracle WebLogic Server"](#)
4. Outbound connections to the LDAP server can originate from Oracle Platform Security Services or from Oracle WebLogic Server:
 - a. [Section 6.5.1.2.1, "Configuring Outbound SSL from Oracle Platform Security Services to LDAP"](#)
 - b. [Section 6.5.1.2.3, "Configuring Outbound SSL from LDAP Authenticator to LDAP"](#)
5. [Section 6.6.1.2, "SSL-Enabling a Data Source"](#)
6. [Section 6.6.1.1, "SSL-Enabling Oracle Database"](#)
7. [Section 6.5.2, "Client-Side SSL for Applications"](#)
8. [Section 6.5.1.2, "Configuring Outbound SSL from Oracle WebLogic Server"](#)
9. [Section 6.6.1.1, "SSL-Enabling Oracle Database"](#)

Keystores and Wallets

Keystores and wallets are central to SSL configuration and are used to store certificates and keys.

For details, see [Section 6.2.2, "Keystores and Oracle Wallets."](#)

6.2.2 Keystores and Oracle Wallets

Oracle Fusion Middleware 12c (12.1.3) supports different types of keystores for keys and certificates:

- JKS-based keystore and truststore

Oracle WebLogic Server uses JKS keystores in upgraded environments.

JDK's `keytool` utility manages JKS keystores and certificates.
- Oracle wallet

System components like Oracle HTTP Server use the Oracle wallet.

Use Fusion Middleware Control, or the command-line WLST and `orapki` interfaces, to manage wallets and their certificates for system components. You can use either the Fusion Middleware Control or WLST to SSL-enable the listeners for these components.

- OPSS Keystore Service (KSS) keystore and truststore

The Keystore Service provides an alternative mechanism to manage keys and certificates. Oracle WebLogic Server uses KSS keystores out-of-the-box in new 12c (12.1.3) installations.

Use Fusion Middleware Control or WLST to manage KSS keystores and their certificates. Use the WebLogic console to SSL-enable the listeners for WebLogic servers.

For more information about these types of stores, and when to use which type of store, see [Section 6.1.3, "Keystores and Wallets"](#).

See Also: [Section 7.1, "Key and Certificate Storage in Oracle Fusion Middleware"](#) for keystore management

JDK7 Requires keyUsage with keyCertSign

Under JDK7, self-signed CA certificates used for SSL configuration must have the keyUsage extension with keyCertSign asserted. For details, see [Section H.3.3](#).

6.2.3 Authentication Modes

The following authentication modes are supported:

- In *no-authentication mode*, neither server nor client are required to authenticate. Other names for this mode include Anonymous SSL/No Authentication/Diffie-Hellman. This mode is considered unsecured.
- In *server authentication mode*, a server authenticates itself to a client. This mode is also referred to as One-way SSL/Server Authentication.
- In *mutual authentication mode*, a client authenticates itself to a server and that server authenticates itself to the client. This mode is also known as Two-way SSL/Client Authentication.
- In *optional client authentication mode*, the server authenticates itself to the client, but the client may or may not authenticate itself to the server. Even if the client does not authenticate itself, the SSL session still goes through.

6.2.4 Tools for SSL Configuration

Oracle Fusion Middleware uses two kinds of configuration tools, common and advanced.

Common Tools

- Fusion Middleware Control
- WLST command-line interface
- Oracle WebLogic Server Administration Console
- `keytool` command-line tool

These tools allow you to configure SSL and manage Oracle Wallet/JKS keystore for any listener or component in Oracle Fusion Middleware.

The first three tools on this list are usable when the component is associated with the application server domain (when the component is not a stand-alone installation).

Advanced Tools

orapki command-line tool is needed to manage wallets for certain stand-alone installations.

See Also: [Section 7.1, "Key and Certificate Storage in Oracle Fusion Middleware"](#) for keystore management

6.3 Configuring SSL for Configuration Tools

Several tools are available for Oracle Fusion Middleware configuration. This section describes how to configure SSL for these tools to enable them to connect to an SSL-enabled Oracle WebLogic Server.

See Also: [Section 6.5.1.1](#) for details about enabling inbound SSL on Oracle WebLogic Server.

For a list of all the configuration tools, see [Section 6.2.4, "Tools for SSL Configuration."](#)

This section contains these topics:

- [Oracle Enterprise Manager Fusion Middleware Control](#)
- [Oracle WebLogic Server Administration Console](#)
- [WLST Command-Line Tool](#)

6.3.1 Oracle Enterprise Manager Fusion Middleware Control

Take these steps:

- Ensure that the SSL port is enabled on the Oracle WebLogic Server instance on which Fusion Middleware Control is deployed, and that the browser (from which you will launch Fusion Middleware Control) trusts the server certificate.

For details, see *Administering Oracle WebLogic Server with Fusion Middleware Control*.

- Now launch Fusion Middleware Control using an SSL-based URL, in the format `https://host:port`.

6.3.2 Oracle WebLogic Server Administration Console

Ensure that the SSL port is enabled on the Oracle WebLogic Server instance. Now launch the administration console by providing the SSL port in the URL. You may get a warning that the certificate is not trusted; accept this certificate and continue.

For details, see *Administering Oracle WebLogic Server with Fusion Middleware Control*.

6.3.3 WLST Command-Line Tool

For details about configuring SSL for WLST, take these steps:

1. Launch the WLST shell.
2. Execute the WLST command:

```
help('connect')
```

Follow the instructions described in the help text to set up the WLST shell in SSL mode.

See Also: [Section 6.9](#) for details about using WLST.

6.4 Configuring SSL for the Web Tier

This section describes SSL for Oracle HTTP Server which resides in the Web tier, and contains these topics:

- [Configuring Load Balancers](#)
- [Enabling SSL for Oracle HTTP Server Virtual Hosts](#)

Note:

- This discussion applies to the Web Tier in the context of an Oracle WebLogic Server domain.
 - The order in which these topics appear should not be confused with the sequence in which SSL is enabled (which varies depending on topology). Rather, they are arranged in order starting with the most front-ending component.
-
-

This chapter does not cover all Oracle HTTP Server configuration options. For additional scenarios, see *Installing and Configuring Oracle HTTP Server*.

6.4.1 Configuring Load Balancers

Use the instructions specific to your load-balancing device to configure load balancers in your Oracle Fusion Middleware environment.

6.4.2 Enabling SSL for Oracle HTTP Server Virtual Hosts

This section shows how to manage SSL configuration for Oracle HTTP Server virtual hosts operating in an Oracle WebLogic Server environment.

Note: For Oracle HTTP Server in standalone mode, see *Administering Oracle HTTP Server*.

For inbound traffic, see:

- [Section 6.4.2.1](#) (using Fusion Middleware Control)
- [Section 6.4.2.2](#) (using WLST)

For outbound traffic, see:

- [Section 6.4.2.3](#) (using either Fusion Middleware Control or WLST)

6.4.2.1 Enabling SSL for Inbound Requests to Oracle HTTP Server Virtual Hosts Using Fusion Middleware Control

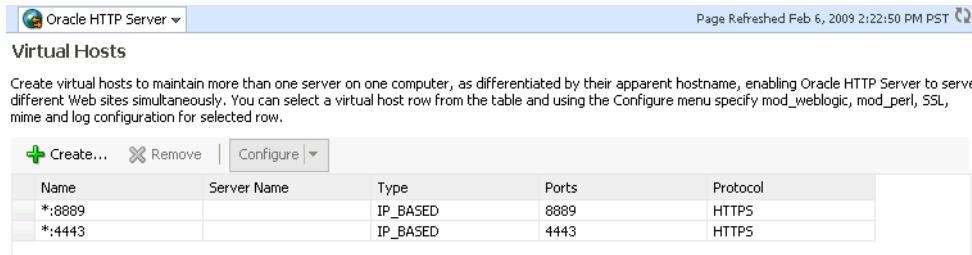
You can SSL-enable inbound traffic to Oracle HTTP Server virtual hosts using these steps:

1. Select the Oracle HTTP Server instance in the navigation pane on the left.
2. Create a wallet, if necessary, by navigating to **Oracle HTTP Server**, then **Security**, then **Wallets**.

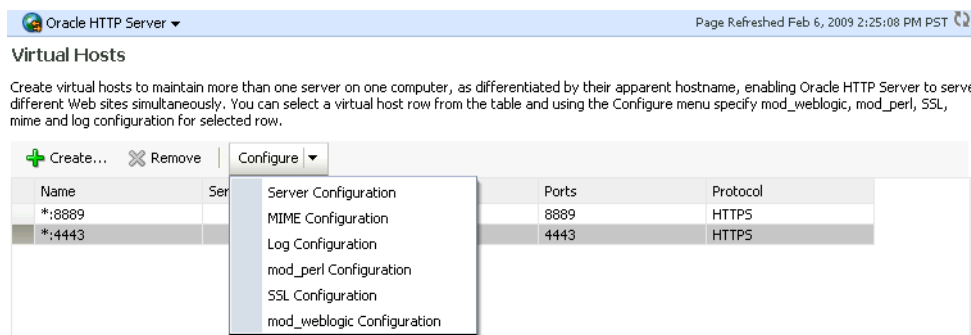
For details about wallet creation and maintenance, see [Chapter 7, "Managing Keystores, Wallets, and Certificates"](#).

3. Navigate to **Oracle HTTP Server**, then **Administration**, then **Virtual Hosts**.

This page shows what hosts are currently configured, and whether they are configured for http or https.



4. Select the virtual host you wish to update, and click **Configure**, then **SSL Configuration**. (Note: If creating a new virtual host, see *Administering Oracle HTTP Server*.)

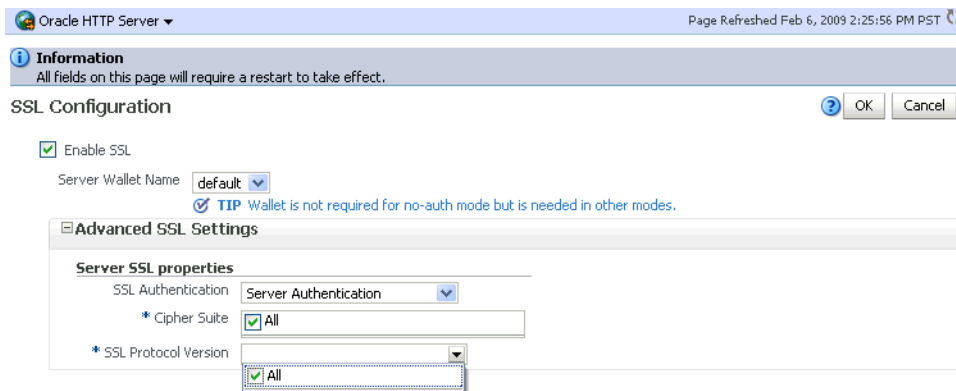


The SSL Configuration page appears.

5. You can convert an https port to http by simply unchecking **Enable SSL**.

To configure SSL for a virtual host that is currently using http:

- Check the **Enable SSL** box.
- Select a wallet from the drop-down list.



- From the Server SSL properties, select the SSL authentication type, cipher suites to use, and the SSL protocol version.

Note: The default values are appropriate in most situations.

Note: ■ This assumes that the certificate is available in Fusion Middleware Control. If it was created through orapki, import it first as explained in [Section 7.4.4.5.1](#).

- The choice of authentication type determines the available cipher suites, and the selected cipher suites determine the available protocol versions. For more information about ciphers and protocol versions, see "Properties Files for SSL" in *Infrastructure Security WLST Command Reference*.
-
-

6. Click **OK** to apply the changes.
7. On Windows platforms only, open Windows Explorer and navigate to your cwallet.sso file. Under properties, security, add SYSTEM in "group or user names".
8. Restart the Oracle HTTP Server instance by navigating to **Oracle HTTP Server**, then **Control**, then **Restart**.
9. Open a browser session and connect to the port number that was SSL-enabled.

6.4.2.2 Enabling SSL for Inbound Requests to Oracle HTTP Server Virtual Hosts Using WLST

Execute these WLST commands using the protocol described in [Section 7.2.1](#).

Take these steps:

1. Determine the virtual hosts for this Oracle HTTP Server instance by running the following command:

```
listListeners('OHS_instance', 'OHS_instance' )
```

This command lists all the virtual hosts for this instance. Select the one that needs to be configured for SSL. For example, you can select vhost1. For details about this command, see *WLST Command Reference for WebLogic Server*.

2. Configure the virtual host with SSL properties:

```
configureSSL('OHS_instance',
'OHS_instance',
'ohs',
'vhost1')
```

Note:

- `configureSSL` uses defaults for all SSL attributes; see "Default Values of Parameters" in *Infrastructure Security WLST Command Reference* for details.
 - You could also specify a properties file as a parameter to `configureSSL`. See "Parameters in Properties File" and "`configureSSL`" in the *Infrastructure Security WLST Command Reference* for details and examples of how to use a properties file. See "`configureSSL`" in the same document for details about this command.
-
-

3. On Windows platforms only, open Windows Explorer and navigate to your `cwallet.sso` file. Under properties, security, add `SYSTEM` in "group or user names".

6.4.2.3 Enabling SSL for Outbound Requests from Oracle HTTP Server

You enable SSL for outbound requests from Oracle HTTP Server by configuring `mod_wl_ohs`.

6.4.2.3.1 Enabling One-Way SSL

The steps are as follows:

1. Generate a custom keystore for Oracle WebLogic Server (see [Section 6.5.1](#)) containing a certificate.
2. Import the trusted CA certificate used by Oracle WebLogic Server into the Oracle HTTP Server wallet as a trusted certificate. You can use any available utility such as WLST or Fusion Middleware Control for this task. (*Note:* The wallet mentioned here is the one that the Oracle HTTP Server listen port uses for SSL. The trusted (root) CA certificate that signed the Oracle WebLogic Server certificate must exist in this wallet. For details on importing trusted certificates see [Section 7.4.7.3.1](#).)
3. With Oracle WebLogic Server instance shut down, edit the Oracle HTTP Server configuration file `DOMAIN_HOME/config/fmwconfig/components/OHS/instance_name/ssl.conf` and add the following line to the SSL configuration under `mod_weblogic`:

```
WlSSLWallet "${DOMAIN_HOME}/config/fmwconfig/components/COMPONENT_TYPE/COMPONENT_NAME/keystores/default"
```

where `default` is the name of the Oracle HTTP Server wallet in Step 2.

Here is an example of how the configuration should look:

```
<IfModule mod_weblogic.c>
WebLogicHost myweblogic.server.com
WebLogicPort 7002
MatchExpression *.jsp
SecureProxy On
WlSSLWallet "${DOMAIN_HOME}/config/fmwconfig/components/OHS/ohs1/keystores/default"
</IfModule>
```

Save the file and exit.

4. On Windows platforms only, open Windows Explorer and navigate to your `cwallet.sso` file. Under properties, security, add `SYSTEM` in "group or user names".
5. Restart Oracle HTTP Server to activate the changes. See *Administering Oracle HTTP Server* for details.
6. Ensure that your Oracle WebLogic Server instance is configured to use the custom keystore generated in Step 1, and that the alias points to the alias value used in generating the certificate. Restart the Oracle WebLogic Server instance. For details, see [Section 6.5.1.1](#).

6.4.2.3.2 Enabling Two-Way SSL

`mod_wl_ohs` also supports two-way SSL communication. To configure two-way SSL:

1. Perform Steps 1 through 4 of the preceding procedure for one-way SSL.
2. Generate a trust store, `trust.jks`, for Oracle WebLogic Server.

The keystore created for one-way SSL (Step 1 of the preceding procedure) could also be used to store trusted certificates, but it is recommended that you create a separate truststore for this procedure.

3. Export the user certificate from the Oracle HTTP Server wallet, and import it into the truststore created in Step 2.

You can use any available utility such as WLST or Fusion Middleware Control for export, and the `keytool` utility for import. For details, see [Section 7.4.5](#).

4. From the Oracle WebLogic Server Administration Console, select the **Keystores** tab for the server being configured.
5. Set the custom trust store with the `trust.jks` file location of the trust store that was created in Step 2 (use the full name).
6. Set the keystore type as JKS, and set the passphrase used to create the keystore.
7. Under the **SSL** tab, ensure that Trusted Certificate Authorities is set as **from Custom Trust Keystore**.
8. Ensure that Oracle WebLogic Server is configured for two-way SSL. For details, see "Configuring SSL" in *Administering Security for Oracle WebLogic Server*.

6.5 Configuring SSL for the Middle Tier

Using SSL in the middle tier includes:

- SSL-enabling the application server
- SSL-enabling components and applications running on the application server

This section addresses mid-tier SSL configuration and contains these topics:

- [Configuring SSL for Oracle WebLogic Server](#)
- [Client-Side SSL for Applications](#)

6.5.1 Configuring SSL for Oracle WebLogic Server

This section describes configuration for the application server.

6.5.1.1 Configuring Inbound SSL to Oracle WebLogic Server

For information and details about implementing SSL to secure Oracle WebLogic Server, see the following topics in *Administering Security for Oracle WebLogic Server*:

- "Configuring Oracle OPSS Keystore Service "
- "Overview of Configuring SSL in WebLogic Server"

6.5.1.2 Configuring Outbound SSL from Oracle WebLogic Server

This section describes how to SSL-enable outbound connections from Oracle WebLogic Server.

- [Configuring Outbound SSL from Oracle Platform Security Services to LDAP](#)
- [Configuring Outbound SSL from Oracle Platform Security Services to Oracle Database](#)
- [Configuring Outbound SSL from LDAP Authenticator to LDAP](#)
- [Configuring Outbound SSL to the Database](#)

6.5.1.2.1 Configuring Outbound SSL from Oracle Platform Security Services to LDAP This section explains how to configure SSL (needs server- and client-side) for policy store and credential store connections to an LDAP directory. It supports anonymous and one-way SSL.

See *Securing Applications with Oracle Platform Security Services* for details about the `jps-config.xml` file referenced in this section.

Anonymous SSL (Server-side)

Start the LDAP server in anonymous authentication mode.

Consult your LDAP server documentation for information on this task.

Anonymous SSL (Client-side)

In your `jps-config.xml` file, you must set the protocol to `ldaps` and specify the appropriate port for the property `ldap.url`. This information needs to be updated for policy store, credential store, key store and any other service instances that use `ldap.url`.

One-Way SSL (Client-side)

The following must be in place for the client-side configuration:

1. The JVM needs to know where to find the trust store that it uses to trust certificates from LDAP. You do this by setting:

```
-Djavax.net.ssl.trustStore=path_to_jks_file
```

This property is added either to the JavaSE program, or to the server start-up properties in a JavaEE environment.
2. In your `jps-config.xml` file, you must set the protocol to `ldaps` and specify the appropriate port for the property `ldap.url`. This information needs to be updated for policy store, credential store, key store and any other service instances that use `ldap.url`.
3. Using **keytool**, import the LDAP server's certificate into the trust store specified in step 1.

6.5.1.2.2 Configuring Outbound SSL from Oracle Platform Security Services to Oracle Database

You can set up a one-way or two-way SSL connection to a database-based OPSS security store.

For details about configuring the database server and clients, see *Securing Applications with Oracle Platform Security Services*.

6.5.1.2.3 Configuring Outbound SSL from LDAP Authenticator to LDAP For details about outbound SSL to LDAP directories, see "How SSL Certificate Validation Works in WebLogic Server" in *Administering Security for Oracle WebLogic Server*.

6.5.1.2.4 Configuring Outbound SSL to the Database See "Configuring Secure Sockets Layer Authentication" in the *Oracle Advanced Security Administrator's Guide* at http://docs.oracle.com/cd/E11882_01/network.112/e10746/asossl.htm for more information about configuring SSL for the database listener.

6.5.2 Client-Side SSL for Applications

For information on how to write SSL-enabled applications, see "Using SSL Authentication in Java Clients" in *Developing Applications with the WebLogic Security Service*.

For best practices, refer to [Section 6.8.2, "Best Practices for Application Developers."](#)

6.6 Configuring SSL for the Data Tier

This section contains this topic:

- [Configuring SSL for the Database](#)

6.6.1 Configuring SSL for the Database

This section contains these topics:

- [SSL-Enabling Oracle Database](#)
- [SSL-Enabling a Data Source](#)

6.6.1.1 SSL-Enabling Oracle Database

Take these steps to SSL-enable Oracle database:

1. Create a root CA and a certificate for the DB. Here is an example:

Note: Self-signed certificates are not recommended for production use. For information about obtain production wallets, see [Section 7.4.8.3, "Changing a Self-Signed Wallet to a Third-Party Wallet."](#)

```
mkdir root
mkdir server

# Create root wallet, add self-signed certificate and export
orapki wallet create -wallet ./root -pwd password
orapki wallet add -wallet ./root -dn CN=root_test,C=US -keysize 2048 -self_
signed -validity 3650 -pwd password
orapki wallet display -wallet ./root -pwd password
orapki wallet export -wallet ./root -dn CN=root_test,C=US -cert
./root/b64certificate.txt -pwd password

#Create server wallet, add self-signed certificate and export
orapki wallet create -wallet ./server -pwd password
orapki wallet add -wallet ./server -dn CN=server_test,C=US -keysize 2048 -pwd
password
orapki wallet display -wallet ./server -pwd password
orapki wallet export -wallet ./server -dn CN=server_test,C=US -request
./server/creq.txt -pwd password

# Import trusted certificates
orapki cert create -wallet ./root -request ./server/creq.txt -cert
./server/cert.txt -validity 3650 -pwd password
orapki cert display -cert ./server/cert.txt -complete
orapki wallet add -wallet ./server -trusted_cert -cert
./root/b64certificate.txt -pwd password
orapki wallet add -wallet ./server -user_cert -cert ./server/cert.txt -pwd
```

```
password
orapki wallet create -wallet ./server -auto_login -pwd password}}
```

2. Update listener.ora, sqlnet.ora, and tnsnames.ora for the database.

a. This example shows the default listener.ora:

```
SID_LIST_LISTENER =
(SID_LIST =(SID_DESC =(SID_NAME = PLSExtProc) (ORACLE_HOME = /path_to_O_
H) (PROGRAM = extproc)))
LISTENER =(DESCRIPTION_LIST =(DESCRIPTION =
(ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1))
(ADDRESS = (PROTOCOL = TCP) (HOST = mynode.mycorp.com) (PORT = 1521))
(ADDRESS = (PROTOCOL = TCPS) (HOST = mynode.mycorp.com) (PORT = 2490))
))

WALLET_LOCATION=(SOURCE=(METHOD=FILE) (METHOD_DATA=(DIRECTORY=/wallet_
location)))

SSL_CLIENT_AUTHENTICATION=FALSE}}
```

And here is an updated listener.ora file, illustrating a scenario with no client authentication:

```
SID_LIST_LISTENER =
(SID_LIST =
(SID_DESC =
(GLOBAL_DBNAME = dbname)
(ORACLE_HOME = /path_to_O_H)
(SID_NAME = sid)
)
)

SSL_CLIENT_AUTHENTICATION = FALSE

WALLET_LOCATION =
(SOURCE =
(METHOD = FILE)
(METHOD_DATA =
(DIRECTORY = /wallet_path)
)
)

LISTENER =
(DESCRIPTION_LIST =
(DESCRIPTION =
(ADDRESS = (PROTOCOL = IPC) (KEY = EXTPROC1521))
)
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCP) (HOST = mynode.mycorp.com) (PORT = 1521))
)
(DESCRIPTION =
(ADDRESS = (PROTOCOL = TCPS) (HOST = mycorp.com) (PORT = 2490))
)
)
```

Note that the SSL port has been added.

b. Likewise, a modified sqlnet.ora file may look like this:

```
NAMES.DIRECTORY_PATH= (TNSNAMES, EZCONNECT)
SQLNET.AUTHENTICATION_SERVICES=(BEQ, TCPS, NTS)
```

```

WALLET_LOCATION=(SOURCE=(METHOD=FILE)(METHOD_DATA=(DIRECTORY=/directory)))
SSL_CLIENT_AUTHENTICATION=FALSE

```

- c. A modified `tnsnames.ora` file may look like this:

```

OID =
  (DESCRIPTION =
    (ADDRESS = (PROTOCOL = TCP)(HOST = mynode.mycorp.com)(PORT = 1521))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = mynode.mycorp.com)
    )
  )

SSL =
  (DESCRIPTION =
    (ADDRESS_LIST =
      (ADDRESS = (PROTOCOL = TCPS)(HOST = mynode.mycorp.com)(PORT = 2490))
    )
    (CONNECT_DATA =
      (SERVICE_NAME = mynode.mycorp.com)
      or
      (SID = mynode.mycorp.com)
    )
    (SECURITY=(SSL_SERVER_CERT_DN=\"CN=server_test,C=US\"))
  )

```

3. Test the connection to the database using the new connect string. For example:

```

$ tnsping ssl
$ sqlplus username/password@ssl

```

See Also: The chapter "Configuring Secure Sockets Layer Authentication" in the *Oracle Database Advanced Security Administrator's Guide*.

6.6.1.2 SSL-Enabling a Data Source

Take these steps to configure your data sources on Oracle WebLogic Server to use SSL.

1. Create a truststore and add the root certificate (which is created when SSL-enabling the database) as a trusted certificate to the truststore.
2. In the Oracle WebLogic Server Administration Console, navigate to the **Connection pool** tab of the data source that you are using.

Note: The data source can be an existing source such as an Oracle WebCenter Portal data source, or a new data source. See *Creating a JDBC Data Source in Administering JDBC Data Sources for Oracle WebLogic Server* for details.

The properties you need to specify in the **JDBC Properties** text box depend on the type of authentication you wish to configure.

- If you will require client authentication (two-way authentication):

```

javax.net.ssl.keyStore=..(password of the keystore)
javax.net.ssl.keyStoreType=JKS
javax.net.ssl.keyStorePassword=...(password of the keystore)
javax.net.ssl.trustStore=...(the truststore location on the disk)

```

```
javax.net.ssl.trustStoreType=JKS
javax.net.ssl.trustStorePassword=... (password of the truststore)
```

- If you will require no client authentication:

```
javax.net.ssl.trustStore=... (the truststore location on the disk)
javax.net.ssl.trustStoreType=JKS
javax.net.ssl.trustStorePassword=... (password of the truststore)
```

3. In the URL text box, enter the JDBC connect string. Ensure that the protocol is TCPS and that SSL_SERVER_CERT_DN contains the full DN of the database certificate.

Use the following syntax if tnsnames.ora uses "SERVICE_NAME":

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCPS) (HOST=host-name) (PORT=port-number))) (CONNECT_
DATA=(SERVICE_NAME=service) (SECURITY=(SSL_SERVER_CERT_DN="CN=server_
test,C=US"))))
```

Use the following syntax if tnsnames.ora uses "SID":

```
jdbc:oracle:thin:@(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCPS) (HOST=host-name) (PORT=port-number))) (CONNECT_
DATA=(SID=service) (SECURITY=(SSL_SERVER_CERT_DN="CN=server_test,C=US"))))
```

4. Test and verify the connection. Your data source is now configured to use SSL.

6.7 Advanced SSL Scenarios

This section explains how to handle additional SSL configuration scenarios beyond the basic topologies described earlier:

- [Hardware Security Modules and Accelerators](#)
- [CRL Integration with SSL](#)
- [Oracle Fusion Middleware FIPS 140-2 Settings](#)

For details and examples of the commands used in this section see [Section 6.9](#).

6.7.1 Hardware Security Modules and Accelerators

A Hardware Security Module (HSM) is a physical plug-in card or an external security device that can be attached to a computer to provide secure storage and use of sensitive content.

Note: This discussion applies only to Oracle HTTP Server, which is a system component supporting HSM.

Oracle Fusion Middleware supports PKCS#11-compliant HSM devices that provide a secure storage for private keys.

Take these steps to implement SSL for a component using a PKCS#11 wallet:

1. Install the HSM libraries on the machine where the component is running. This is a one-time task and is device-dependent.
2. Next, create a wallet using the `orapki` command-line tool. Note the following:
 - a. Choose PKCS11 as the wallet type.

- b. Specify the device-specific PKCS#11 library used to communicate with the device. This library is part of the HSM software.

On Linux, the library is located at:

```
For LunaSA (Safenet): /usr/lunasa/lib/libCryptoki2.so
For nCipher: /opt/nfast/toolkits/pkcs11/libcknfast.so
```

On Windows, the library is located at:

```
For LunaSA (Safenet): C:\Program Files\LunaSA\cryptoki.dll
```

3. Now follow the standard procedure for obtaining third-party certificates: create a certificate request; get the request approved by a Certificate Authority (CA); and install the certificate signed by that CA.

The wallet you set up is used like any other wallet.

4. Verify the wallet with the `orapki` utility. Use the following command syntax:

```
orapki wallet p11_verify [-wallet [wallet]] [-pwd password]
```

See Also: [Appendix G, "orapki"](#) for details about `orapki`

5. Configure SSL on your component listener using the `configureSSL WLST` command, providing a properties file as input. Your properties file should specify the full path of the PKCS#11 wallet directory on the machine where the component is running. (*Note:* Do not save the PKCS#11 wallet in the instance home directory. Only wallets created and managed through Fusion Middleware Control or WLST should reside in the instance home.)

A sample properties file could look like this:

```
SSLEnabled=true
AuthenticationType=Server
PKCS11Wallet=/tmp/lunasa/wallet
```

Note: You must use the WLST command `configureSSL` to configure the PKCS11 wallet. You cannot do this task using Fusion Middleware Control or any other tool.

6.7.2 CRL Integration with SSL

Note:

- This discussion applies only to Oracle HTTP Server in the context of an Oracle WebLogic Server environment. For SSL configuration in standalone components, see *Administering Oracle HTTP Server*.
 - Manage CRL validation through WLST. You cannot perform this task through Fusion Middleware Control.
-
-

Components that use SSL can optionally turn on certificate validation using a certificate revocation list (CRL). This allows them to validate the peer certificate in the SSL handshake and ensure that it is not on the list of revoked certificates issued by the Certificate Authority (CA).

This section describes how to configure a component to use CRL-based validation, and how to create and set up CRLs on the file system.

6.7.2.1 Configuring CRL Validation for a Component

Configure SSL on your component listener using the `configureSSL WLST` command, providing a properties file as input.

The properties file must be set up as follows:

1. The `CertValidation` attribute must be set to `url`.
2. The `CertValidationPath` attribute must be of the form `file://file_path` or `dir://directory_path`.
 - Use the first format if you are using a single CRL file for certificate validation. This CRL file should contain a concatenation of all CRLs.
 - Use the second format if you are specifying a directory path that contains multiple CRL files in hashed form.

See [Section 6.7.2.2, "Manage CRLs on the File System"](#) on how to create CRLs in hashed form.

In this example, the properties file specifies a single CRL file:

```
SSLEnabled=true
AuthenticationType=Server
CertValidation=crl
KeyStore=ohs1
CertValidationPath=file:///tmp/file.crl
```

In this example, the properties file specifies a directory path to multiple CRL files:

```
SSLEnabled=true
AuthenticationType=Server
KeyStore=ohs1
CertValidation=crl
CertValidationPath=dir:///tmp
```

6.7.2.2 Manage CRLs on the File System

Note: LDAP-based CRLs or CRL distribution points are not supported.

You use the `orapki` command-line tool to manage CRLs on the file system. For details on this topic, see [Section G.1.5, "Managing Certificate Revocation Lists \(CRLs\) with orapki Utility."](#)

CRL Renaming to Hashed Form

If specifying a CRL storage location, the CRL must be renamed. This enables CRLs to be loaded in an efficient manner at runtime. This operation creates a symbolic link to the actual CRL file. On Windows, it copies the CRL to a file with a new name.

To rename a CRL:

```
orapki crl hash
[-crl [url|filename]] [-wallet wallet] [-symlink directory]
[-copy directory] [-summary] [-pwd password]
```

For example:

```
orapki crl hash -crl nzcrl.txt -symlink wltldir -pwd password
```

If the CRL file name is specified at runtime, multiple CRLs can be concatenated in that file. The CRL created in this example is in Base64 format, and you can use a text editor to concatenate the CRLs.

CRL Creation

Note: CRL creation and Certificate Revocation are for test purposes and only used in conjunction with self-signed certificates. For production use, obtain production certificates from well-known CAs and obtain the CRLs from those authorities.

To create a CRL:

```
orapki crl create
[-crl [url|filename]] [-wallet [cawallet]] [-nextupdate [days]] [-pwd password]
```

For example:

```
orapki crl create
-crl nzcrl.crl -wallet rootwlt -nextupdate 3650 -pwd password
```

Certificate Revocation

Revoking a certificate adds the certificate's serial number to the CRL.

To revoke a certificate:

```
orapki crl revoke
[-crl [url|filename]] [-wallet [cawallet]] [-cert [revokecert]] [-pwd password]
```

For example:

```
orapki crl revoke
-crl nzcrl.txt -wallet rootwlt -cert cert.txt -pwd password
```

6.7.2.3 Test a Component Configured for CRL Validation

To test that a component is correctly configured for CRL validation, take these steps:

1. Set up a wallet with a certificate to be used in your component.
2. Generate a CRL with this certificate in the revoked certificates list. Follow the steps outlined in [Section 6.7.2.2, "Manage CRLs on the File System."](#)
3. Configure your component to use this CRL. Follow the steps outlined in [Section 6.7.2.1, "Configuring CRL Validation for a Component."](#)
4. The SSL handshake should fail when this revoked certificate is used.

6.7.3 Oracle Fusion Middleware FIPS 140-2 Settings

For details about FIPS 140 support in Oracle Fusion Middleware, see [Chapter 8](#).

6.8 Best Practices for SSL

This section outlines some best practices for Oracle Fusion Middleware component administrators and application developers. It contains these topics:

- [Best Practices for Administrators](#)
- [Best Practices for Application Developers](#)

6.8.1 Best Practices for Administrators

Best practices for system administrators include the following:

- Use self-signed wallets only in test environment. You should obtain a CA signed certificate in the wallet before moving to production environment. For details, see [Chapter 7, "Managing Keystores, Wallets, and Certificates."](#)
- It is recommended that components (at least in the Web tier) use certificates that have the system host name or virtual host or site name as the DN. This allows browsers to connect in SSL mode without giving unsettling warning messages.
- A minimum key size of 1024 bits is recommended for certificates used for SSL. Higher key size provides more security but at the cost of reduced performance. Pick an appropriate key size value depending on your security and performance requirements.
- Lack of trust is one of the most common reasons for SSL handshake failures. Ensure that the client trusts the server (by importing the server CA certificate into the client keystore) before starting SSL handshake. If client authentication is also required, then the reverse should also be true.

6.8.2 Best Practices for Application Developers

The following practices are recommended:

- Use Java Key Store (JKS) to store certificates for your Java EE applications.
- Externalize SSL configuration parameters like keystore path, truststore path, and authentication type in a configuration file, rather than embedding these values in the application code. This allows you the flexibility to change SSL configuration without having to change the application itself.

6.9 WLST Reference for SSL

WLST commands are available to manage Oracle wallets and to configure SSL for Oracle Fusion Middleware components.

See the following chapters of the *Infrastructure Security WLST Command Reference* for details about these WLST commands:

- "SSL Configuration WLST Commands"
- "Wallet Configuration WLST Commands"

See Also: [Section 7.2, "Command-Line Interface for Keystores and Wallets"](#) for important instructions on how to launch the WLST shell to run SSL-related commands. Do not launch the WLST interface from any other location.

Note: All WLST commands for SSL configuration must be run in online mode.

Note: WLST allows you to import certificates only in PEM format.

Managing Keystores, Wallets, and Certificates

This chapter explains how to use Oracle Fusion Middleware security features to administer keystores, keys, and certificates. These artifacts are used to configure SSL and related tasks for Oracle Fusion Middleware components.

This chapter contains these sections:

- [Section 7.1, "Key and Certificate Storage in Oracle Fusion Middleware"](#)
- [Section 7.2, "Command-Line Interface for Keystores and Wallets"](#)
- [Section 7.3, "Keystore Management"](#)
- [Section 7.4, "Wallet Management"](#)

7.1 Key and Certificate Storage in Oracle Fusion Middleware

Keys and certificates are used to digitally sign and verify data and achieve authentication, integrity, and privacy in network communications.

Private keys, digital certificates, and trusted CA certificates are stored in keystores. This section describes the keystores available in Oracle Fusion Middleware and contains these topics:

- [Types of Keystores](#)
- [Keystore Management Tools](#)

7.1.1 Types of Keystores

Oracle Fusion Middleware provides various types of keystores for keys and certificates as shown in [Table 7-1](#):

Table 7-1 Keystore Types in Oracle Fusion Middleware

Keystore Type	Description	Protection Mechanism
Oracle Wallet	Oracle Wallet	Password or auto-login
JKS	Java Keystore	Password
KSS	OPSS Keystore Service	Password or policy

7.1.1.1 About Oracle Wallet

An Oracle wallet is a container that stores your credentials, such as certificates, trusted certificates, certificate requests, and private keys. You can store Oracle wallets on the

file system or in LDAP directories such as Oracle Internet Directory. Oracle wallets can be auto-login or password-protected wallets.

When creating a wallet, you can:

- Pre-populate it with a self-signed certificate. Such a wallet is called a test wallet and is typically used in development and testing phases.
- Create a certificate request, so that you can request a signed certificate back from a Certificate Authority (CA). Once the CA sends the certificate back, it is imported into the wallet. Such a wallet is called a third-party wallet.

Either the test wallet or the third-party wallet may be password-protected, or may be configured to not require a password, in which case it is called an auto-login wallet.

Oracle Wallets are used for Oracle HTTP Server. As of Oracle Fusion Middleware 12c (12.1.3), you can take advantage of the central storage and unified management available with the Keystore Service to manage wallets and their contents through the export, import, and synchronization features of that service.

See Also:

- [Section 7.1.1.3](#) for more information on the Keystore Service;
- *Infrastructure Security WLST Command Reference* for details about the `importKeyStore`, `exportKeyStore`, and `syncKeyStore` commands.

7.1.1.2 About the JKS Keystore

A JKS keystore is the default JDK implementation of Java keystores. Java EE applications can use the JKS-based keystore and truststore.

7.1.1.3 About the Keystore Service (KSS) Keystore

The OPSS Keystore Service enables you to manage keys and certificates for SSL, message security, encryption, and related tasks.

The Keystore Service offers several advantages including policy-based protection and centralized management of keystores and truststores, expiring certificates, and other key material.

In Oracle Fusion Middleware 12c (12.1.3), Oracle WebLogic Server:

- uses the Keystore Service out-of-the-box
- uses JKS by default in upgraded environments.

7.1.2 Keystore Management Tools

Oracle Fusion Middleware provides these options for keystore operations:

- WLST, a command-line interface for JKS keystores and Oracle wallets
- `orapki`, a command-line tool for wallets
- Fusion Middleware Control, a graphical user interface

About Importing DER-encoded Certificates

You cannot use Fusion Middleware Control or the WLST command-line tool to import DER-encoded certificates or trusted certificates into an Oracle wallet. Use `orapki` command-line tool instead.

Using a Keystore Not Created with WLST or Fusion Middleware Control

If an Oracle wallet was created with tools such as `orapki`, it must be imported prior to use. Specifically for Oracle HTTP Server, if a wallet was created using `orapki`, in order to view or manage it in Fusion Middleware Control you must first import it with either Fusion Middleware Control or the WLST `importWallet` command. For details, see [Section 7.4.4.5.1](#) and [Section 7.4.4.5.2](#).

Copying Keystores to File System Not Supported

Creating, renaming, or copying keystores directly to any directory on the file system is not supported. Any pre-existing keystore or wallet that you wish to use must be imported using either Fusion Middleware Control or the WLST utility.

Managing Wallets in a Stand-alone Environment

In a stand-alone environment, such as a stand-alone OHS installation, the keystore management features are provided by the database.

For details, see *Administering Oracle HTTP Server*:

JDK7 Requirement for Self-Signed Certificates

JDK7 requires the `keyUsage` extension for self-signed CA certificates used for SSL configuration. For details, see [Section H.3.3](#).

Additional Information

Details about the tools are provided in these sections:

- [Command-Line Interface for Keystores and Wallets](#)
- [Wallet Management](#)
- [Appendix G, "orapki"](#)

7.2 Command-Line Interface for Keystores and Wallets

Oracle Fusion Middleware provides a set of WLST scripts to create and manage keystores and Oracle wallets, and to manipulate their stored objects.

7.2.1 How to Launch the Command-Line Interface

When running SSL WLST commands, you must invoke the WLST script from the Oracle Common home. (See [Section 7.2.1](#) for more information.)

This brings up the WLST shell. Connect to a running Oracle WebLogic Server instance by specifying the user name, password, and connect URL. After connecting, you are now ready to run SSL-related WLST commands as explained in the subsequent sections.

Note: All SSL-related WLST commands require you to launch the script from the above-mentioned location only.

Here is the basic execution sequence:

```
./wlst.sh
connect('weblogic','weblogic1') --- To connect to WebLogic Admin Server
editCustom()
startEdit()
wlstCommand('param1', 'param2', 'param3', 'param4')
```

```
save()
activate()
```

where `wlstCommand` is the actual WLST command. For example, to create an OHS wallet:

```
connect('weblogic','weblogic1') --- For connecting to WLS Admin Server
editCustom()
startEdit()
createWallet('ohs1', 'ohs1', 'ohs', 'testwallet')
save()
activate()
```

In this command the first two parameters both refer to the component instance name (in contrast with earlier releases where they referred to an Oracle instance and a component instance respectively, in this release both refer to the latter), the third parameter is the component, and the fourth parameter is the wallet name.

Here is a sample output for `createWallet`:

```
wls:/base_domain/serverConfig> editCustom()
Location changed to edit custom tree. This is a writable tree with No root.
For more help, use help('editCustom')
```

```
wls:/base_domain/editCustom> startEdit()
Starting an edit session ...
Started edit session, please be sure to save and activate your
changes once you are done.
wls:/base_domain/editCustom>
createWallet('ohs1','ohs1','ohs','testwallet','Welcome1')
Wallet created
wls:/base_domain/editCustom> save()
Saving all your changes ...
Saved all your changes successfully.
wls:/base_domain/editCustom> activate()
Activating all your changes, this may take a while ...
The edit lock associated with this edit session is released
once the activation is completed.
Activation completed
```

7.3 Keystore Management

For details about Keystore Service (KSS) keystore management, see "Keystore Management with the Keystore Service" in *Securing Applications with Oracle Platform Security Services*.

7.4 Wallet Management

This section contains the following topics:

- [About Wallets and Certificates](#)
- [Accessing the Wallet Management Page in Fusion Middleware Control](#)
- [Managing the Wallet Life Cycle](#)
- [Common Wallet Operations](#)
- [Managing the Certificate Life Cycle](#)
- [Accessing the Certificate Management Page for Wallets in Fusion Middleware Control](#)

- [Common Certificate Operations](#)
- [Wallet and Certificate Maintenance](#)

This discussion assumes that components are installed within a WebLogic domain. For wallet configuration in a stand-alone context, for example a stand-alone Oracle HTTP Server, see [Appendix G](#).

7.4.1 About Wallets and Certificates

This section contains the following topics:

- [About Password-Protected and Autologin Wallets](#)
- [About Self-Signed and Third-Party Wallets](#)
- [Sharing Wallets Across Instances](#)
- [Wallet Naming Conventions](#)

7.4.1.1 About Password-Protected and Autologin Wallets

You can create two types of wallets:

- Auto-login wallet

This is an obfuscated form of a PKCS#12 wallet that provides PKI-based access to services and applications without requiring a password at runtime. You can also add to, modify, or delete the wallet without needing a password. File system permissions provide the necessary security for auto-login wallets.

Note: In previous releases, you could create a wallet with a password and then enable auto-login to create an obfuscated wallet. With 12c (12.1.3), auto-login wallets are created without a password. When using such a wallet, you do not need to specify a password.

If using an auto-login wallet without a password, specify a null password ("") in the `ldapbind` command.

Older type of wallets (such as Release 10g wallets) will continue to work as they did earlier.

- Password-protected wallet

As the name suggests, this type of wallet is protected by a password. Any addition, modification, or deletion to the wallet content requires a password.

Every time a password-protected wallet is created, an auto-login wallet is automatically generated. However, this auto-login wallet is different from the user-created auto-login wallet described in the previous bullet. While the user-created wallet can be updated at configuration time without a password, an automatically generated auto-login wallet is a read-only wallet that does not allow direct updates. The wallet must be modified through the password protected file (by providing a password), at which time the auto-login wallet is regenerated.

The purpose of this system-generated auto-login wallet is to provide PKI-based access to services and applications without requiring a password at runtime, while still requiring a password at configuration time.

7.4.1.2 About Self-Signed and Third-Party Wallets

Self-signed wallets contain certificates for which the issuer is the same as the subject. These wallets are typically created for use within an intranet environment where trust is not a high priority. Each self-signed wallet has its own unique issuer; hence, in an environment with multiple components and wallets, the trust management tasks increase n-fold.

When created through Fusion Middleware Control, a self-signed wallet is valid for five years.

Third-party wallets contain certificates that are issued by well known Certificate Authorities (CA's). The functionality and security remain the same as for self-signed wallets, but the use of third-party certificates provides added trust because the issuers are well known, so they are already trusted by most clients.

Difference Between Self-Signed and Third-Party Wallets

From a functional and security perspective, a self-signed certificate is comparable to one issued by a third party. The only difference is that a self-signed certificate is not trusted.

7.4.1.3 Sharing Wallets Across Instances

Oracle recommends that you do not share wallets between component instances, since each wallet represents a unique identity.

The exception to this is an environment with a cluster of component instances, in which case wallet sharing would be an acceptable practice.

Note that no management tools or interfaces are available to facilitate wallet sharing. However, you can export a wallet from one instance and import it into another instance. See [Section 7.4.4](#) for details of wallet export and import.

7.4.1.4 Wallet Naming Conventions

Follow these naming conventions for your Oracle wallets:

- Do not use a name longer than 256 characters.
- Do not use any of the following characters in a wallet name:
| ; , ! @ # \$ () < > / \ " ' ` ~ { } [] = + & ^ space tab

Note: Observe this rule even your operating system supports the character.

- Do not use non-ASCII characters in a wallet name.
- Additionally, follow the operating system-specific rules for directory and file names

Due to the way data is handled in an LDAP directory, wallet names are not case-sensitive.

Thus, it is recommended that you use case-insensitive wallet names (preferably, using all lower case letters). For example, if you have created a wallet named `UPPER`, do not create another wallet named `upper`; doing so could cause confusion during wallet management operations.

7.4.1.5 Wallet Requirements in JDK7

JDK7 requires the `keyUsage` extension for self-signed CA certificates used for SSL configuration. For details, see [Section H.3.3](#).

7.4.2 Accessing the Wallet Management Page in Fusion Middleware Control

An Oracle wallet is associated with the component where it is utilized. To locate a component instance:

1. Log into Fusion Middleware Control using administrator credentials.
2. Select the domain of interest.

Note: You can use Setup to discover a specific Oracle WebLogic Server domain to work with.

3. From the navigation pane, locate the instance (for example, an OHS instance) that will use the wallet. Click on the instance.

The component type now appears on the upper left of the page adjacent to the Farm drop-down.

4. Select the component type drop-down (for example, Oracle HTTP Server).

If the component is not started, start it by right-clicking to open the component menu, press **Control**, then **Start Up**.

5. Navigate to **Security**, then **Wallets**.

6. The Wallets page appears.

On the Wallets page, you can:

- Create a wallet.
- Delete a wallet.
- Import a wallet.
- Export a wallet.

7.4.3 Managing the Wallet Life Cycle

Typical life cycle events for an Oracle wallet are as follows:

- The wallet is created. Wallets can be created directly, or by importing a wallet file from the file system.
- The list of available wallets are viewed and specific wallets selected for update.
- Wallets are updated or deleted. Update operations for password-protected wallets require that the wallet password be entered.
- The wallet password can be changed for password-protected wallets.
- The wallet can be deleted.
- Wallets can be exported and imported.

Note: As of Oracle Fusion Middleware 12c (12.1.3), you can take advantage of the central storage and unified console available with the Keystore Service to manage wallets and their contents through the export, import, and synchronization features of that service. See *Infrastructure Security WLST Command Reference* for details about the `importKeyStore`, `exportKeyStore`, and `syncKeyStore` commands.

7.4.4 Common Wallet Operations

This section describes the steps required to perform a range of wallet management functions, including:

- [Creating a Wallet](#)
- [Creating a Self-Signed Wallet](#)
- [Changing a Self-Signed Wallet to a Third-Party Wallet](#)
- [Exporting a Wallet](#)
- [Importing a Wallet](#)
- [Deleting a Wallet](#)

7.4.4.1 Creating a Wallet

This section explains how to create an Oracle wallet:

- [Creating a Wallet Using Fusion Middleware Control](#)
- [Creating a Wallet Using WLST](#)

7.4.4.1.1 Creating a Wallet Using Fusion Middleware Control Take these steps to create a wallet:

1. Navigate to the Wallets page for your component instance. See [Section 7.4.2, "Accessing the Wallet Management Page in Fusion Middleware Control."](#)
2. Click **Create**.
3. The Create Wallet page appears.
4. Enter a wallet name.
5. Check or uncheck the **Autologin** box, depending on whether your wallet will be an auto-login wallet. The default is an auto-login wallet.

See [Section 7.4.1.1, "About Password-Protected and Autologin Wallets"](#) for details.

Note: Wallets configured for Oracle Internet Directory must have auto-login enabled.

6. Click **Submit**.
7. At this point, you must choose whether to add a certificate request (CR) at this time. If you choose not to do so, you can always add the CR later; see [Section 7.4.7.1.1, "Adding a Certificate Request Using Fusion Middleware Control."](#)

In this example, we choose to add a CR:

Note: The common name entered here should match the host name of the Oracle HTTP Server to which clients will connect; this helps to prevent problems of the type mentioned in [Section 7.4.8.2](#).

8. Click **Finish**.
9. There are two options for the CR:
 - Copy and paste the Base64-encoded certificate request from the text box to a file.
 - Export it directly to a file with the **Export Certificate Request** button.
10. A message appears confirming the wallet creation.

7.4.4.1.2 Creating a Wallet Using WLST

Execute these WLST commands using the protocol described in [Section 7.2.1](#).

Assuming the component instance is ohs1, use this command to create a wallet:

```
createWallet('ohs1', 'ohs1', 'ohs', 'ohs2', 'password')
```

where ohs2 is the wallet name and password is the password for this wallet. If an auto-login wallet needs to be created, the password should be specified as "" (that is, no text between the quotes).

See Also: "createWallet" in the *Infrastructure Security WLST Command Reference*.

7.4.4.2 Creating a Self-Signed Wallet

This section explains how to create a self-signed wallet:

- [Creating a Self-Signed Wallet Using Fusion Middleware Control](#)
- [Creating a Self-Signed Wallet Using WLST](#)

7.4.4.2.1 Creating a Self-Signed Wallet Using Fusion Middleware Control

Take these steps to create a self-signed wallet:

See Also: [Section 7.4.1.2, "About Self-Signed and Third-Party Wallets"](#)

1. Navigate to the Wallets page for your component instance. See [Section 7.4.2, "Accessing the Wallet Management Page in Fusion Middleware Control."](#)
2. Click **Create Self-Signed Wallet**.
3. On the Self-Signed Wallet page, enter data to create the wallet. This includes:
 - The wallet name
 - Whether this is an auto-login wallet

See Also: [Section 7.4.1.1, "About Password-Protected and Autologin Wallets"](#)

- The DN information
- The key size

The screenshot shows the 'Create Self-Signed Wallet' page in Oracle Internet Directory. At the top, it says 'Oracle Internet Directory' and 'Page Refreshed Feb 6, 2009 3:13:56 PM PST'. The breadcrumb is 'Wallets > Create Self-Signed Wallet'. There are 'OK' and 'Cancel' buttons. A warning message states: 'A self signed wallet is not signed by a well known CA. A self-signed wallet is not recommended in a production environment. The wallet name should be unique for a given component. The wallet type can be auto-login or password-protected. Passwords, if specified, have a minimum length of eight characters, and contain alphabetic characters combined with numeric or special characters. Auto-login wallet is an obfuscated form of PKCS#12 wallet that provides PKI-based access to services and applications without requiring a password at runtime. Auto-login wallet don't need a password to modify, or delete the wallet. File system permissions provide the necessary security for Auto-login wallets.'

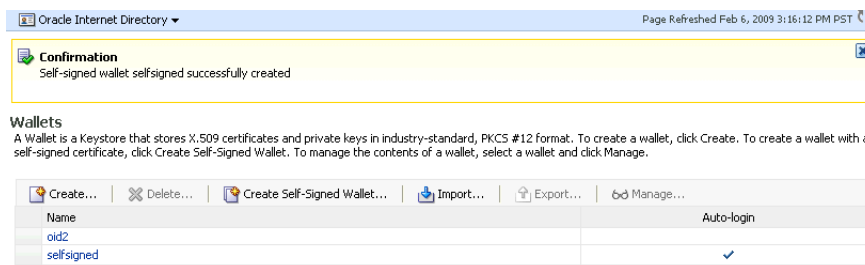
Self-Signed Wallet Details

- * Wallet Name: selfsigned
- Auto-login
- Wallet Password: [text box]
- Confirm Password: [text box]

Add Self-Signed Certificate
Add a self-signed certificate that becomes part of the wallet.

- * Common Name: ldap.acme.com
- Organizational Unit: FOR TESTING ONLY
- Organization: [text box]
- City: [text box]
- State: [text box]
- Country: United States
- Key Size: 1024

4. Click **Submit**.
5. A confirmation message is displayed and the new wallet appears in the list of wallets.



Note: Wallets configured for Oracle Internet Directory must have auto-login enabled.

7.4.4.2.2 Creating a Self-Signed Wallet Using WLST

Execute these WLST commands using the protocol described in [Section 7.2.1](#).

Assuming the component instance is `ohs1`, use these commands to create a self-signed wallet:

```
createWallet('ohs1', 'ohs1', 'ohs', 'ohs2', 'password')
addSelfSignedCertificate('ohs1', 'ohs1', 'ohs', 'ohs2', 'password', 'subject_dn',
'key_size')
```

where `ohs2` is the wallet name, `subject_dn` is the distinguished name of the self-signed certificate, `key_size` is the key size in bits and `password` is the password for this wallet. If an auto-login wallet needs to be created, the password should be specified as "" (that is, with no text between the quotes).

See Also:

- "createWallet" in the *Infrastructure Security WLST Command Reference*
- "addSelfSignedCertificate" in the *Infrastructure Security WLST Command Reference*.

Note: Wallets configured for Oracle Internet Directory must have auto-login enabled.

7.4.4.3 Changing a Self-Signed Wallet to a Third-Party Wallet

For steps to convert a self-signed wallet into a third-party wallet, see [Section 7.4.8.3](#), "[Changing a Self-Signed Wallet to a Third-Party Wallet](#)."

7.4.4.4 Exporting a Wallet

This section explains how to export a wallet:

- [Exporting a Wallet Using Fusion Middleware Control](#)
- [Exporting a Wallet Using WLST](#)

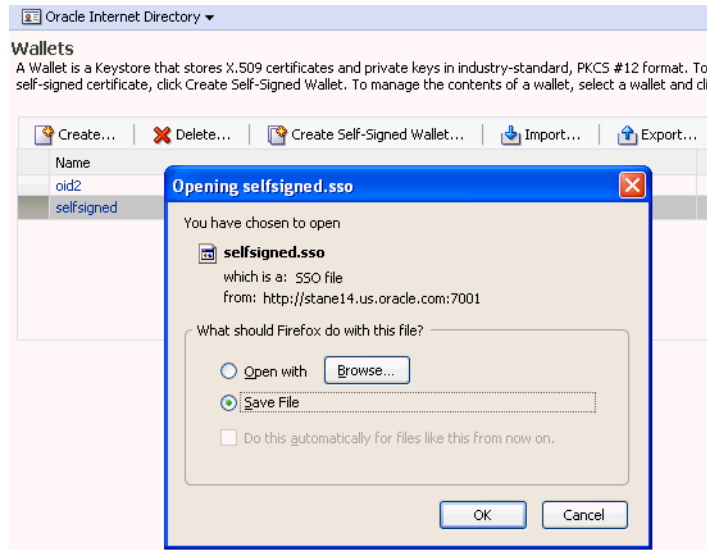
7.4.4.4.1 Exporting a Wallet Using Fusion Middleware Control Take these steps to export a wallet:

1. Navigate to the Wallets page for your component instance. See [Section 7.4.2](#), "[Accessing the Wallet Management Page in Fusion Middleware Control](#)."

2. Select the row corresponding to the wallet of interest.

Note: Do not click on the wallet name itself; this opens the wallet for certificate management operations.

3. Click **Export**.
4. The Export Wallet page appears.
5. Enter the filename and the location where the wallet is to be exported.
6. Click **OK**.



7.4.4.4.2 Exporting a Wallet Using WLST

Execute these WLST commands using the protocol described in [Section 7.2.1](#).

Assuming the component instance is `ohs1`, use this command to export a wallet:

```
exportWallet('ohs1', 'ohs1', 'ohs', 'selfsigned', 'password', '/tmp')
```

where `password` is the password for this wallet (specify `"` as password for auto-login wallet).

If it is an auto-login wallet, this command will export the wallet into a file named `cwallet.sso` under the directory `/tmp`. If it is a password-protected wallet, there will be two files created under `/tmp`, namely `ewallet.p12` and `cwallet.sso`.

See Also: "exportWallet" in the *Infrastructure Security WLST Command Reference*.

7.4.4.5 Importing a Wallet

This section explains how to import a wallet:

- [Importing a Wallet Using Fusion Middleware Control](#)
- [Importing a Wallet Using WLST](#)

7.4.4.5.1 Importing a Wallet Using Fusion Middleware Control

Take these steps to import a wallet:

1. Navigate to the Wallets page for your component instance. See [Section 7.4.2, "Accessing the Wallet Management Page in Fusion Middleware Control"](#).
2. Click **Import**.
3. The Import Wallet page appears.
4. If this is an auto-login wallet, check the box and enter the wallet name. No password is required.

Oracle Internet Directory Page Refreshed Feb 6, 2009 3:18:30 PM PST

Wallets > Import Wallet

Import Wallet OK Cancel

Click "Browse" to select the wallet and import it for the selected component. The wallet name should be unique for the component. Password-protected wallet files usually have a ".p12" extension and auto-login wallets have a ".sso" extension. You import a wallet to use for a component, for example with SSL operations.

File:

Auto-login

* Wallet Name:

Wallet Password:

5. If this is not an auto-login wallet, uncheck the auto-login box. Specify both the wallet name and password.

Oracle Internet Directory Page Refreshed Feb 6, 2009 3:18:30 PM PST

Wallets > Import Wallet

Import Wallet OK Cancel

Click "Browse" to select the wallet and import it for the selected component. The wallet name should be unique for the component. Password-protected wallet files usually have a ".p12" extension and auto-login wallets have a ".sso" extension. You import a wallet to use for a component, for example with SSL operations.

File:

Auto-login

* Wallet Name:

* Wallet Password:

6. Click **OK**. The wallet is imported into the repository.

7.4.4.5.2 Importing a Wallet Using WLST

Execute these WLST commands using the protocol described in [Section 7.2.1](#).

Assuming the component instance is `ohs1`, use this command to import a wallet:

```
importWallet('ohs1', 'ohs1', 'ohs', 'ohs5', 'password', '/tmp/ewallet.p12')
```

where `ohs5` is the wallet name, `password` is the password of the wallet being imported and `/tmp/ewallet.p12` contains the wallet file (if there are two files `ewallet.p12` and `cvwallet.sso`, point to `ewallet.p12`). Point to `cvwallet.sso` only if it is an auto-login wallet - in this case, the password should be specified as "".

See Also: "importWallet" in the *Infrastructure Security WLST Command Reference*.

7.4.4.6 Deleting a Wallet

This section explains how to delete a wallet:

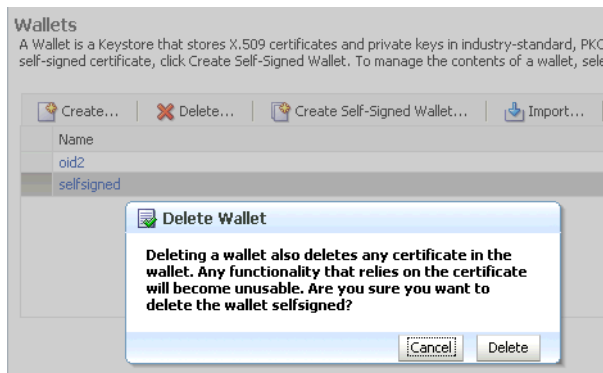
- [Deleting a Wallet Using Fusion Middleware Control](#)
- [Deleting a Wallet Using WLST](#)

7.4.4.6.1 Deleting a Wallet Using Fusion Middleware Control

Take these steps to delete a wallet:

1. Navigate to the Wallets page for your component instance. See [Section 7.4.2, "Accessing the Wallet Management Page in Fusion Middleware Control."](#)

2. Select the row corresponding to the wallet of interest.
3. Click **Delete**.



4. The wallet is deleted and no longer appears on the list of wallets.

7.4.4.6.2 Deleting a Wallet Using WLST

Execute these WLST commands using the protocol described in [Section 7.2.1](#).

Assuming the component instance is `ohs1`, use this command to delete a wallet:

```
deleteWallet('ohs1', 'ohs1', 'ohs', 'selfsigned')
```

See Also: "deleteWallet" in the *Infrastructure Security WLST Command Reference*.

7.4.5 Managing the Certificate Life Cycle

The complete certificate life cycle, starting from wallet creation, includes these actions:

1. Create an empty wallet (that is, a wallet that does not contain a certificate request).
2. Add a certificate request to the wallet.
3. Export the certificate request.
4. Use the certificate request to obtain the corresponding certificate.
5. Import trusted certificates.
6. Import the certificate.

These steps are needed to generate a wallet with a third-party trusted certificate. For details about this task, see [Section 7.4.7.5.1, "Converting a Self-Signed Certificate into a Third-Party Certificate Using Fusion Middleware Control."](#)

See Also: [Section 7.4.6, "Accessing the Certificate Management Page for Wallets in Fusion Middleware Control"](#)

7.4.6 Accessing the Certificate Management Page for Wallets in Fusion Middleware Control

An Oracle wallet is associated with the component where it is utilized.

To locate a component instance:

1. Log into Fusion Middleware Control using administrator credentials.
2. Select the domain of interest.

Note: You can use Setup to discover a specific Oracle WebLogic Server domain to utilize.

3. Use the navigation pane to locate the instance (for example, an Oracle HTTP Server instance) that will use the wallet. *Note:* Oracle HTTP Server must be running so that subsequent steps will work.

After locating your component instance, there are two ways you can access a wallet's certificate management page in Fusion Middleware Control:

- Go to the *Wallets* page, select the line for the wallet of interest and click **Manage**.
- Go to the *Wallets* page, locate the wallet of interest, and click on the wallet name.

On the Certificate Management page, you can:

- Add a certificate request.
- Export a certificate request, a certificate, or a trusted certificate.
- Import a certificate or a trusted certificate.
- Delete a certificate request, a certificate, or a trusted certificate.

7.4.7 Common Certificate Operations

This section describes the following common certificate operations:

- [Adding a Certificate Request](#)
- [Exporting a Certificate, Certificate Request, or a Trusted Certificate](#)
- [Importing a Certificate or a Trusted Certificate](#)
- [Deleting a Certificate Request, a Certificate, or a Trusted Certificate](#)
- [Converting a Self-Signed Certificate into a Third-Party Certificate](#)

7.4.7.1 Adding a Certificate Request

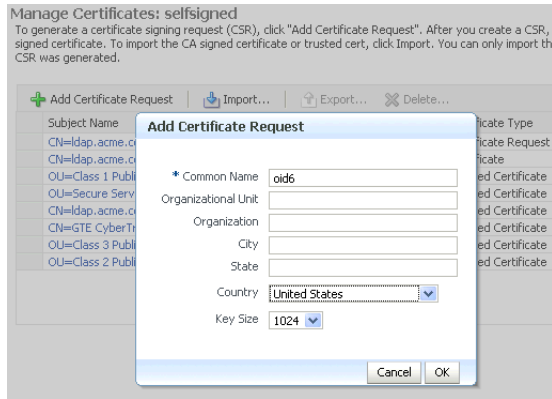
This section explains how to add a certificate request to a wallet:

- [Adding a Certificate Request Using Fusion Middleware Control](#)
- [Adding a Certificate Request Using WLST](#)

7.4.7.1.1 Adding a Certificate Request Using Fusion Middleware Control

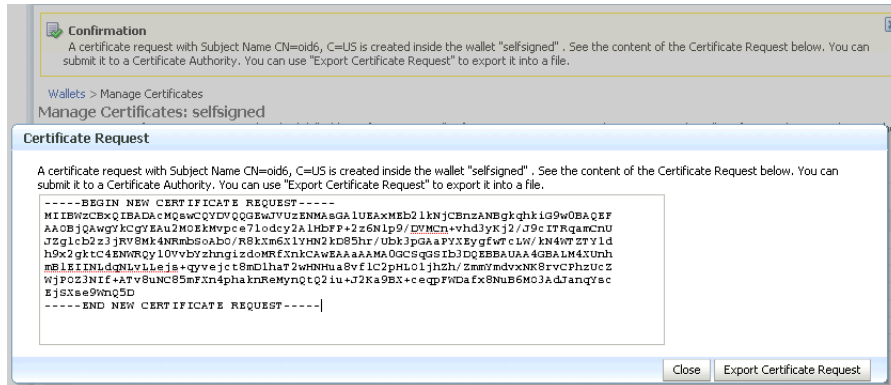
It is possible to add a certificate request at the time you create the wallet, but if it was not done at that time, you can do so using the following steps:

1. Navigate to the Certificate Management page. See [Section 7.4.6, "Accessing the Certificate Management Page for Wallets in Fusion Middleware Control."](#)
2. Click **Add Certificate Request**.
3. A dialog box appears where you enter the CRs DN values:



Fields marked with an asterisk (*) are required. *Note:* The common name must be the host name that clients will use to access the component.

4. Click **OK**.
5. The new CR is generated and a dialog box appears with the CR in the text box. You can either:
 - Copy and paste the Base64-encoded certificate request to a file.
 - Export it directly to a file with the **Export Certificate Request** button.



7.4.7.1.2 Adding a Certificate Request Using WLST

Execute these WLST commands using the protocol described in [Section 7.2.1](#).

Assuming the component instance is `ohs1`, use this command to add a certificate request for a wallet:

```
addCertificateRequest('ohs1', 'ohs1', 'ohs', 'selfsigned', 'password', 'subject_dn', 'key_size')
```

where `password` is the password for this wallet, `subject_dn` is the distinguished name by which the certificate request is generated and `key_size` is the key size in bits.

See Also: "addCertificateRequest" in the *Infrastructure Security WLST Command Reference*.

7.4.7.2 Exporting a Certificate, Certificate Request, or a Trusted Certificate

This section explains how to export a Certificate, Certificate Request, or a Trusted Certificate:

- [Exporting a Certificate, Certificate Request, or a Trusted Certificate Using Fusion Middleware Control](#)
- [Exporting a Certificate, Certificate Request, or a Trusted Certificate Using WLST](#)

7.4.7.2.1 Exporting a Certificate, Certificate Request, or a Trusted Certificate Using Fusion Middleware Control Take these steps to export a certificate, a certificate request (CR), or a trusted certificate:

1. Navigate to the Certificate Management page. See [Section 7.4.6, "Accessing the Certificate Management Page for Wallets in Fusion Middleware Control."](#)
2. Select the certificate, CR, or trusted certificate and click **Export**.
3. A dialog box appears with the certificate, CR, or trusted certificate in the text box. You can either:
 - Copy and paste the Base64-encoded certificate to a file.
 - Export it directly to a file with the **Export Certificate** or **Export Trusted Certificate** button.

7.4.7.2.2 Exporting a Certificate, Certificate Request, or a Trusted Certificate Using WLST Execute these WLST commands using the protocol described in [Section 7.2.1](#).

Assuming the component instance is `ohs1`, use this command to export a certificate request:

```
exportWalletObject('ohs1', 'ohs1', 'ohs', 'selfsigned', 'password',
'CertificateRequest', '/tmp', 'subject_dn')
```

where `password` is the password for this wallet, `/tmp` is the path under which the certificate request is exported in BASE64 format in the file `base64.txt`, and `subject_dn` is the distinguished name of the certificate request that is exported.

To export a certificate or trusted certificate, replace `CertificateRequest` in the above command with `Certificate` or `TrustedCertificate`.

See Also: "exportWalletObject" in the *Infrastructure Security WLST Command Reference*.

7.4.7.3 Importing a Certificate or a Trusted Certificate

This section explains how to import a Certificate or a Trusted Certificate:

- [Importing a Certificate or a Trusted Certificate Using Fusion Middleware Control](#)
- [Importing a Certificate or a Trusted Certificate Using WLST](#)

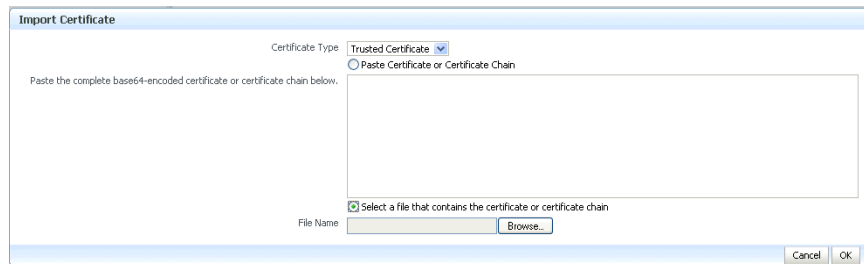
7.4.7.3.1 Importing a Certificate or a Trusted Certificate Using Fusion Middleware Control

Note: You cannot use Fusion Middleware Control to import DER-encoded certificates or trusted certificates into an Oracle wallet. Use `orapki` command-line tool instead.

Take these steps to import a certificate or a trusted certificate:

1. Navigate to the Certificate Management page. See [Section 7.4.6, "Accessing the Certificate Management Page for Wallets in Fusion Middleware Control."](#)
2. Click **Import**.

3. In the Import Certificate dialog, you can select either a certificate or a trusted certificate.
4. There are two ways to do the import:
 - Paste the Base64-encoded certificate or trusted certificate in the text box.
 - Use the file selector to browse your file system to locate a file containing the Base64-encoded certificate or trusted certificate.



5. Click OK.

7.4.7.3.2 Importing a Certificate or a Trusted Certificate Using WLST

Note: You cannot use the WLST command-line tool to import DER-encoded certificates or trusted certificates into an Oracle wallet. Use `orapki` command-line tool instead.

Execute these WLST commands using the protocol described in [Section 7.2.1](#).

Assuming the component instance is `ohs1`, use this command to import a certificate into a wallet:

```
importWalletObject('ohs1', 'ohs1', 'ohs', 'selfsigned', 'password', 'Certificate',
'/tmp/cert.txt')
```

where `password` is the password for this wallet and `/tmp/cert.txt` is the file that contains BASE64 encoded certificate.

To import a trusted certificate, replace `Certificate` in the above command with `TrustedCertificate`.

See Also: "importWalletObject" in the *Infrastructure Security WLST Command Reference*.

7.4.7.4 Deleting a Certificate Request, a Certificate, or a Trusted Certificate

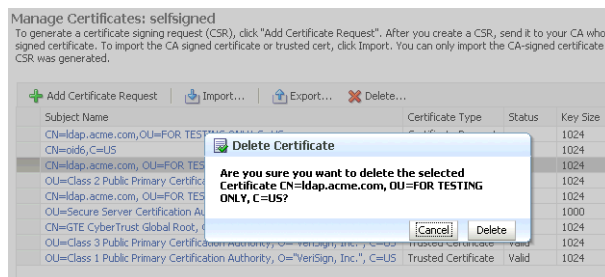
This section explains how to delete a Certificate Request, a Certificate, or a Trusted Certificate:

- [Deleting a Certificate Request, a Certificate, or a Trusted Certificate Using Fusion Middleware Control](#)
- [Deleting a Certificate Request, a Certificate, or a Trusted Certificate Using WLST](#)

7.4.7.4.1 Deleting a Certificate Request, a Certificate, or a Trusted Certificate Using Fusion Middleware Control

Take these steps to delete a CR, a certificate, or a trusted certificate:

1. Navigate to the Certificate Management page. See [Section 7.4.6, "Accessing the Certificate Management Page for Wallets in Fusion Middleware Control."](#)
2. Select the row containing the certificate request, certificate or trusted certificate.
3. Click **Delete**.
4. A dialog box appears, requesting confirmation.



5. Click **Yes**.
6. The object no longer appears in the Manage Certificates list.

7.4.7.4.2 Deleting a Certificate Request, a Certificate, or a Trusted Certificate Using WLST

Execute these WLST commands using the protocol described in [Section 7.2.1](#).

Assuming the component instance is `ohs1`, use this command to delete a certificate:

```
removeWalletObject('ohs1', 'ohs1', 'ohs', 'selfsigned', 'password', 'Certificate',
'subject_dn')
```

where `password` is the password for this wallet and `subject_dn` is the distinguished name of the certificate being deleted.

To delete a certificate request or trusted certificate, replace `Certificate` in the above command with `CertificateRequest` or `TrustedCertificate`.

See Also: "removeWalletObject" in the *Infrastructure Security WLST Command Reference*.

7.4.7.5 Converting a Self-Signed Certificate into a Third-Party Certificate

This section explains how to convert a Self-Signed Certificate into a Third-Party Certificate:

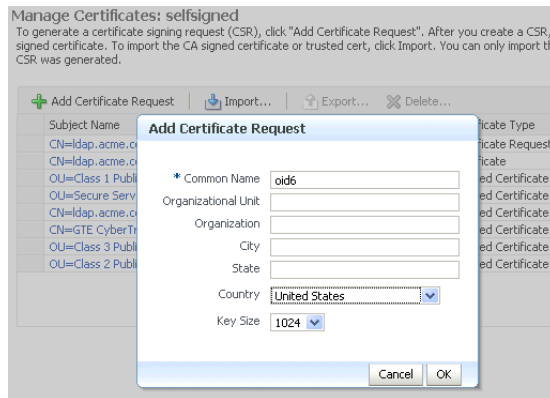
- [Converting a Self-Signed Certificate into a Third-Party Certificate Using Fusion Middleware Control](#)
- [Converting a Self-Signed Certificate into a Third-Party Certificate Using WLST](#)

7.4.7.5.1 Converting a Self-Signed Certificate into a Third-Party Certificate Using Fusion Middleware Control

A self-signed certificate residing in a wallet can be converted into a third-party certificate signed by a certificate authority (CA). Take these steps to perform the task:

Note: The steps are illustrated for use with Oracle Internet Directory, and similar steps are applicable for generating wallets to use with Oracle HTTP Server.

1. From the navigation pane, locate your component instance.
2. Navigate to *component_name*, then **Security**, then **Wallets**.
3. From the list of wallets, select the wallet that contains the self-signed certificate.
4. The Manage Certificates page appears. It contains the list of certificates in the wallet.
5. A new certificate request must be generated for the self-signed certificate that is to be converted. Select the self-signed certificate and click **Add Certificate Request**. A dialog box appears:



Note: The common name entered here should match the host name of the server to which clients will connect; this helps to prevent problems of the type mentioned in [Section 7.4.8.2](#).

6. Enter the certificate request (CR) details and click **OK**.
The CR is generated. You can either:
 - Copy and paste the Base64-encoded certificate request to a file.
 - Export it directly to a file with the **Export Certificate Request** button.
7. Submit the certificate request file to a certificate authority to generate a certificate. This is an offline procedure that you can execute in accordance with your local policy for obtaining certificates.
8. The CA signs the certificate request and generates a certificate. The CA will return you one of the following:
 - A single file containing both the newly generated certificate and its own CA certificate in *pkcs7* format
 - Multiple files, one of which will be the newly generated certificate and the other(s) its own CA certificate (or certificates, if there is a chain)
9. Use **Import** to import these files into your wallet:
 - If you received a single file from the CA, import it as a trusted certificate, using an alias that matches the alias of the self-signed certificate you are replacing (from Step 3).
 - If you received two or more files:
 - Import the file(s) containing the CA certificate or certificate chain as trusted certificate(s) (use an alias that is unique in the wallet).

- Import the certificate file as a certificate (using an alias that matches the alias of the self-signed certificate you are replacing).

Note: The order is important: you must import the trusted certificate first, followed by the certificate.

For more information on how to identify the correct Trusted CA Certificate or the correct chain of Trusted CA certificates, see Doc ID 1368940.1 in My Oracle Support Knowledge Base
<https://support.oracle.com/epmos/faces/DocumentDisplay?id=1368940.1>

The CA returned a single file, which is imported as a trusted certificate:

10. After import, the certificate issued by the CA replaces the self-signed certificate.

7.4.7.5.2 Converting a Self-Signed Certificate into a Third-Party Certificate Using WLST

See Also: [Section 6.9](#)

Execute these WLST commands using the protocol described in [Section 7.2.1](#).

Follow these steps to convert a self signed certificate to a third-party certificate using WLST:

1. Add a certificate request, for example:

```
addCertificateRequest('inst1', 'ohs1', 'ohs', 'selfsigned', 'password',
'subject_dn', 'key_size')
```

2. Export the certificate request:

```
exportWalletObject('inst1', 'ohs1', 'ohs', 'selfsigned', 'password',
'CertificateRequest', '/tmp', 'subject_dn')
```

3. Submit the certificate request `/tmp/base64.txt` to a certificate authority. The CA will return a newly generated certificate and its own certificate, either as one file in PKCS#7 format or as multiple files, one of which will be the newly generated certificate and the other(s) its own CA certificate (or certificates, if there is a chain).
4. If you receive a single file from the CA, run the following command:

```
importWalletObject('inst1', 'ohs1', 'ohs', 'selfsigned', 'password',
'TrustedChain', '/tmp/cert.txt')
```

where `password` is the password for this wallet and `/tmp/cert.txt` is the file that the CA returned and contains BASE64 encoded PKCS#7.

If you receive two or more files from the CA, import the file(s) containing the CA certificate or certificate chain as trusted certificate(s) first, followed by the newly generated certificate. For example when two files are returned:

```
importWalletObject('inst1', 'ohs1', 'ohs', 'selfsigned', 'password',  
'TrustedCertificate', '/tmp/cacert.txt')
```

```
importWalletObject('inst1', 'ohs1', 'ohs', 'selfsigned', 'password',  
'Certificate', '/tmp/cert.txt')
```

where `password` is the password for this wallet, `/tmp/cert.txt` is the file that the CA returned and contains BASE64 encoded certificate and `/tmp/cacert.txt` is the file containing the BASE64 encoded CA certificate.

For more information on how to identify the correct Trusted CA Certificate or the correct chain of Trusted CA certificates, see Doc ID 1368940.1 in My Oracle Support Knowledge Base

<https://support.oracle.com/epmos/faces/DocumentDisplay?id=1368940.1>

See Also: The following references in the *Infrastructure Security WLST Command Reference*:

- "addCertificateRequest"
- "exportWalletObject"
- "importWalletObject".

7.4.8 Wallet and Certificate Maintenance

This section contains the following administration topics:

- [Location of Wallets](#)
- [Effect of Host Name Change on a Wallet](#)
- [Changing a Self-Signed Wallet to a Third-Party Wallet](#)
- [Replacing an Expiring Certificate in a Wallet](#)

7.4.8.1 Location of Wallets

This section describes the location of wallets and provides maintenance details.

Root Directory for an Oracle HTTP Server Wallet

The root directory for Oracle HTTP Server wallets is:

```
$DOMAIN_HOME/config/fmwconfig/components/OHS/ohs_instance_name/keystores
```

This root directory contains subdirectories with wallet names, and these subdirectories contain the actual wallet files.

For example, assuming `ohs_instance1` contains two wallets named `ohs1` and `ohs2`, respectively. `ohs1` is a password-protected wallet, and `ohs2` is an auto-login-only wallet. A sample structure could look like this:

```
$DOMAIN_HOME/config/fmwconfig/components/OHS/ohs_instance1  
/keystores/ohs1/cwallet.sso
```

```
$DOMAIN_HOME/config/fmwconfig/components/OHS/ohs_instance1  
/keystores/ohs1/ewallet.p12
```

```
$DOMAIN_HOME/config/fmwconfig/components/OHS/ohs_instance1  
/keystores/ohs2/cwallet.sso
```

7.4.8.2 Effect of Host Name Change on a Wallet

Typically, the wallet DN is based on the host name of the server where the wallet is used.

For example, if a wallet is being created for the Oracle HTTP Server my.example.com, then the DN of the certificate in this Oracle HTTP Server wallet will be something like "CN=my.example.com,O=organization name".

This synchronization is required because most clients do host name verification during the SSL handshake.

Clients that perform host name verification include Web browsers and Oracle HTTPClient, among others. If the host name of the server does not match that of the certificate DN, then:

- A clear warning will be displayed (in the case of browser clients).
- There may be SSL handshake failure (in the case of other clients).

Thus, when you have a wallet on a server that is accepting requests from clients, you must ensure that whenever the host name of this server changes, you also update the certificate in the wallet.

You can do this by requesting a new certificate with a new DN (based on the new host name).

7.4.8.2.1 Requesting a New Certificate for a Production Wallet

The steps are:

- Generate a new request with the new DN (based on new host name).
- Send this request to a certificate authority (CA).
- Get back a new certificate from the CA.
- Delete the older certificate and certificate request from the wallet.
- Import the new certificate.

See [Section 7.4.4](#) for details about these operations.

7.4.8.2.2 Requesting a New Certificate for a Self-signed Wallet

The steps are:

- Delete the existing wallet.
- Create a new wallet with a self-signed certificate using the new DN (based on the new host name).

See [Section 7.4.4](#) for details about these operations.

For both production and self-signed wallets, once the new certificate is available in the wallet, you need to ensure that it is imported into all the component wallets where it needs to be trusted. For example, if Oracle WebLogic Server is SSL-enabled and the certificate for Oracle WebLogic Server changed due to a host name change, then you need to import its new certificate into the Oracle HTTP Server wallet so that it can trust its new peer.

7.4.8.3 Changing a Self-Signed Wallet to a Third-Party Wallet

You can convert a self-signed wallet into a third-party wallet, one that contains certificates signed by a trusted Certificate Authority (CA).

Assuming a self-signed wallet named `MYWallet`, containing a certificate with DN as `"CN=my.example.com,O=example"`, take these steps to convert it into a third-party wallet:

1. Remove the user certificate `"CN=my.example.com,O=example"` from the wallet.
2. Remove the trusted certificate `"CN=my.example.com,O=example"` from the wallet (this has the same DN as the user certificate, but is a separate entity nonetheless).
3. Export the certificate request `"CN=my.example.com,O=example"` from the wallet and save it to a file.
4. Give this certificate request file to a third-party certificate authority (CA) such as Verisign.
5. The CA will return one of the following:
 - A user certificate file and its own certificate file
 - A single file with a certificate chain consisting of a user certificate and its own certificate
6. Import the above file(s) into the wallet.

See [Section 7.4.4](#) for details about these operations.

7.4.8.4 Replacing an Expiring Certificate in a Wallet

An expiring certificate should be replaced before it actually expires to avoid or reduce application downtime.

The steps for replacing an expiring certificate are as follows:

1. Export the certificate request from the wallet (this is the same request for which the current expiring certificate was issued).
2. Provide this certificate request to the third-party Certificate Authority (CA) for certificate issuance. The validity date of the new certificate should be earlier than the expiration date of the current certificate. This overlap is recommended to reduce downtime.

Note: Steps 1 and 2 are not required when the third-party CA already maintains the certificate request in a repository. In that case, simply request the CA to issue a new certificate for that certificate request.

3. Remove the existing certificate (the one that is about to expire) from the wallet.
4. Import the newly issued certificate into the wallet.

To reduce downtime, remove the previous certificate and import the new certificate in the overlap period when the new certificate has become valid and the older one has not yet expired.

5. If the new certificate was issued by a CA other than the one that issued the original certificate, you may also need to import the new CA's trusted certificate before importing the newly issued certificate.

See [Section 7.4.4](#) for details about these operations.

FIPS 140 Support in Oracle Fusion Middleware

This chapter describes Oracle Fusion Middleware support for FIPS 140.

This chapter contains these topics:

- [Section 8.1, "About the FIPS Standard"](#)
- [Section 8.2, "About FIPS 140 in Oracle Fusion Middleware Release 12c \(12.1.3\)"](#)
- [Section 8.3, "Components with FIPS 140 Support"](#)
- [Section 8.4, "Common Scenarios for an Operational FIPS 140 Environment"](#)
- [Section 8.5, "Troubleshooting FIPS 140 Issues"](#)

8.1 About the FIPS Standard

Federal Information Processing Standards (FIPS) are a series of standards established by the US National Institute of Standards for Technology (NIST) for use in evaluating the security of computer systems and networks.

One of the FIPS standards, FIPS 140-2, specifies the security requirements that must be met by a cryptographic module to protect sensitive information. The standard provides four increasing, qualitative levels of security to cover the wide range of potential applications and environments in which cryptographic modules may be employed.

Note: In the remainder of this chapter, the term 'FIPS 140' refers to the FIPS 140-2 standard.

8.2 About FIPS 140 in Oracle Fusion Middleware Release 12c (12.1.3)

Oracle Fusion Middleware Release 12c (12.1.3) supports the use of FIPS 140-enabled cryptographic libraries.

The ability to operate in FIPS 140 mode is **not** a generic, product suite-wide claim. Instead, it is specific to a defined set of scenarios and transactions supported by relevant Oracle Fusion Middleware 12c (12.1.3) product components. It applies where validated cryptography is used to support or enforce security-sensitive tasks such as authentication, authorization, confidentiality, integrity, and so on.

The use of cryptographic services for other tasks that are non-security sensitive does not require FIPS 140 compliance. Oracle Fusion Middleware 12c (12.1.3) supports

enabling FIPS 140 mode for security-sensitive scenarios while complying and co-existing with product functionality that does not require operating in that mode.

About FIPS 140-validated Libraries

To support FIPS 140 operation, Oracle Fusion Middleware 12c (12.1.3) includes FIPS 140-validated RSA libraries from RSA, the Security Division of EMC (RSA). Algorithms not approved under FIPS 140 are disabled within the RSA libraries.

The libraries are based on RSA version 6.1 BSAFE and JCE software and include the following modules:

- Crypto-J V6.1.1
- SSL-J V6.1.2
- Cert-J V6.1.1

Note: These are the FIPS 140-certified library and module versions at the time of publication. The actual versions in effect at your installation could be slightly different from the ones listed here, as the vendor may issue some patches between certification and the time the product actually shipped. Thus the actual version could be a dot release of the certified version.

The version number is for information only; you can do any independent verification of certification and strength of algorithms.

For background about the FIPS 140 standards and algorithms, refer to the FIPS 140-2 documentation at:

<http://csrc.nist.gov/publications/PubsFIPS.html>

Provider and Algorithm Selection

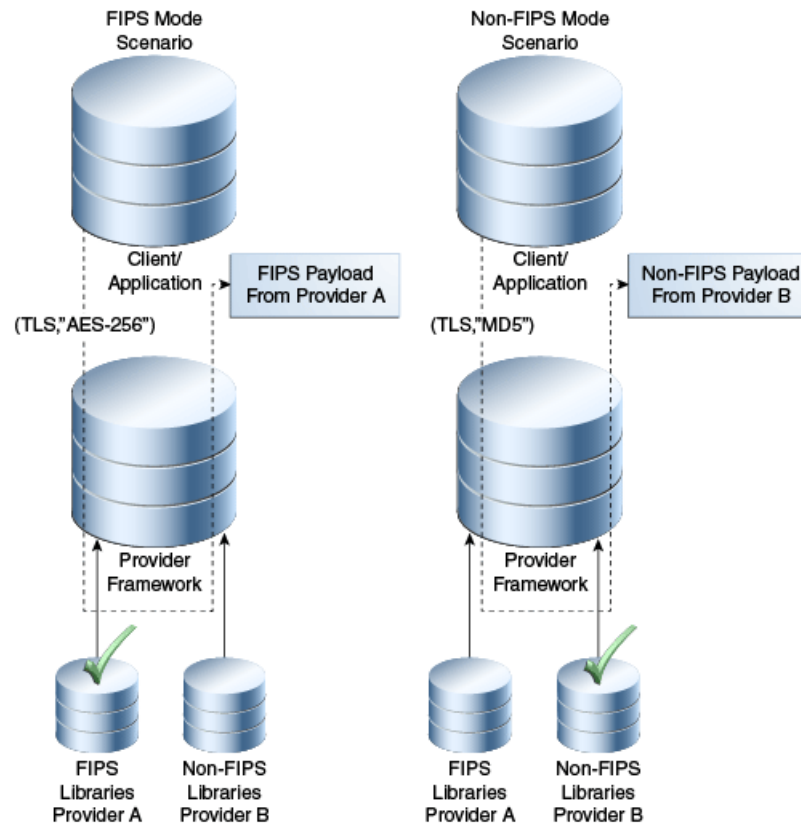
FIPS 140 implementation in Oracle Fusion Middleware occurs in the context of the Java platform's Java Cryptography Architecture (JCA). To accommodate the co-existence of FIPS 140-validated algorithms for security-sensitive tasks as well as algorithms for other tasks, additional cryptographic providers are also configured to provide functionality not supported in FIPS 140-validated RSA libraries, and for certain non-compliant cryptographic functions such as MD5, which are disabled within the FIPS 140-validated RSA libraries.

The basic flow is as follows:

- An application (for example, an external web client or Oracle HTTP Server) requests a service or connection to a server such as WebLogic Server. The request typically involves a "payload" such as a data packet to be transmitted.
- JCA evaluates the request to determine whether FIPS 140 compliance is required.
- The request is routed to JCA's "provider" framework, which contains a set of (FIPS 140-compliant and non-compliant) providers for digital signatures, message digests (hashes), certificates, and certificate validation, encryption, and other cryptographic services.
- The providers are searched in preference order and the implementation from the first provider that supplies the correct algorithm is returned. For the security-sensitive cases, only FIPS 140 compliant algorithms are used to execute the cryptographic operations.

Figure 8–1 illustrates this flow:

Figure 8–1 Selecting a FIPS 140 Provider



- The first request, on the left, is made in a security-sensitive scenario. JCA uses the SHA-256 provider from the RSA cryptographic library to process the request and deliver the FIPS 140 payload.
- The second request, on the right, is executed in a non-sensitive scenario. JCA uses the MD5 provider from the non-cryptographic library to process the request with the non-FIPS 140 payload.

Thus, a security-sensitive scenario such as HTTPS/TLS inbound and outbound communication which is intended to be FIPS 140-compliant uses only those cryptographic functions available in the FIPS 140-validated RSA libraries to encrypt and sign HTTPS/TLS network payloads.

8.3 Components with FIPS 140 Support

When you plan to work with FIPS 140 in Oracle Fusion Middleware, be aware of the different components at various layers of the middleware stack where certain features may operate in FIPS 140 mode. If any component in the stack is operating in non-FIPS 140 mode, the transaction may not be FIPS 140-compliant. It is therefore important to ensure that all relevant components are operating in FIPS 140 mode.

Table 8–1 lists the components where you can enable FIPS 140, and contains the following details:

- The Oracle Fusion Middleware layer where the component resides;

- the component name
- the scenario which can be FIPS 140-enabled
- cross-reference to product documentation for details, including how to enable or disable FIPS 140, other relevant configuration details, and what product functions support the use of FIPS 140-validated cryptography.

Note: Not all features of each listed component are FIPS 140-compliant. Only the specified features support FIPS 140.

Table 8–1 Components with FIPS 140 Support in Oracle Fusion Middleware

Component Layer	Component	Feature	Details
Fusion Middleware Core	Oracle HTTP Server	<ul style="list-style-type: none"> ■ TLS Inbound (HTTPS) ■ TLS Outbound from OHS to WLS 	These topics in <i>Administering Oracle HTTP Server</i> : <ul style="list-style-type: none"> ■ "SSLFIPS" directive for mod_ossll ■ "Managing Application Security"
	Oracle WebLogic Server	<ul style="list-style-type: none"> ■ TLS inbound: HTTPS, T3S, JMX/T3S, JMS ■ TLS outbound: HTTPS, T3S, JMX/T3S, JMS, JDBC (Oracle RDBMS) ■ Database Connections (through Data Source) 	"Enabling FIPS Mode" in <i>Administering Security for Oracle WebLogic Server</i> "Use the SHA-256 Secure Hash Algorithm" in <i>Securing WebLogic Web Services for Oracle WebLogic Server</i> "Using Encrypted Connection Properties" in <i>Administering JDBC Data Sources for Oracle WebLogic Server</i>
	Oracle Platform Security Services	<ul style="list-style-type: none"> ■ Keystore Service ■ Credential Store Service 	"FIPS Support in OPSS" in <i>Securing Applications with Oracle Platform Security Services</i>
	Oracle Web Services Manager	<ul style="list-style-type: none"> ■ Message protection ■ Token signature 	"Supported Algorithm Suites" in <i>Securing Web Services and Managing Policies with Oracle Web Services Manager</i>
Database	Oracle Database	<ul style="list-style-type: none"> ■ Database in FIPS 140 mode 	"Oracle Database FIPS 140-2 Settings" in <i>Oracle Database Security Guide</i>

Note: Database is included for reference. Consult the certification matrix for supported versions and other details.

8.4 Common Scenarios for an Operational FIPS 140 Environment

Table 8–1 listed the components in Oracle Fusion Middleware with FIPS 140 features. Table 8–2 lists typical protocols for each component scenario:

Note: These are representative scenarios - the table is not intended to provide a comprehensive listing of all possible scenarios.

Table 8–2 FIPS 140 Scenarios

Feature or Connection	Communication Protocol	Signature Algorithm/Protocol Details
Inbound connection from an external web client or application to Oracle HTTP Server	<ul style="list-style-type: none"> ▪ HTTPS (Client Access to OHS) ▪ SOAP-TLS (Server to Server Communication) 	HTTPS Server (TLS, Mutual Authentication, RSA-2048 with SHA-256 X.509 Certificates, AES-256 Bulk Data Encryption)
Outbound connection from Oracle HTTP Server to Oracle WebLogic Server	<ul style="list-style-type: none"> ▪ HTTPS (OHS to HTTP Servlet in WLS) for end-end SSL with external SSL termination in OHS. 	HTTPS Client (TLS, Mutual Authentication, RSA-2048 with SHA-256 X.509 Certificates, AES-256 Bulk Data Encryption)
Inbound connection from an external web client or application to Oracle WebLogic Server	<ul style="list-style-type: none"> ▪ HTTPS (Client Access to HTTP Servlet) ▪ SOAP-TLS (Server to Server Communication) 	HTTPS Server (TLS, Mutual Authentication, RSA-2048 with SHA-256 X.509 Certificates, AES-256 Bulk Data Encryption)
Outbound connection from Oracle WebLogic Server to an external web, proxy or application server	<ul style="list-style-type: none"> ▪ HTTPS (WLS to an external HTTPS server) ▪ SOAP-TLS (Server to Server Communication) 	HTTPS Client (TLS, Mutual Authentication, RSA-2048 with SHA-256 X.509 Certificates, AES-256 Bulk Data Encryption)
Outbound connection from Oracle WebLogic Server to Oracle Database 11gR2	<ul style="list-style-type: none"> ▪ DB-TLS-jdbc (WebLogic to Database Communication) 	JDBC (TLS, Mutual Authentication, RSA-2048 with SHA-256 X.509 Certificates, AES-256 Bulk Data Encryption)
XML Message Protection (XML Signing) for SOAP messages using Oracle Web Services Manager	<ul style="list-style-type: none"> ▪ SOAP-MsgSec 	XML Signature (Basic256Sha256, Basic256Sha256Rsa15); Entire Body, Include SwA Attachment
XML Message Protection (XML Encryption) for SOAP messages using Oracle Web Services Manager	<ul style="list-style-type: none"> ▪ SOAP-MsgSec 	XML Signature (Basic256Sha256, Basic256Sha256Rsa15); Entire Body, Include SwA Attachment
Inbound JMS connection to Oracle WebLogic Server	<ul style="list-style-type: none"> ▪ JMS traffic is secure in flight 	JMS/TLS
Outbound JMS connection from Oracle WebLogic Server	<ul style="list-style-type: none"> ▪ JMS traffic is secure in flight 	JMS/TLS
Secure JNDI lookups from deployed components	<ul style="list-style-type: none"> ▪ JDNI-EJB 	T3S
Secure administrator access to servers	<ul style="list-style-type: none"> ▪ WLST traffic to WLS server is secure in flight 	T3S
Keystore and Certificate Generation	<ul style="list-style-type: none"> ▪ Encryption ▪ Key Exchange 	RSA 2048, AES 256, SHA-2
Hashing Algorithms, Password-Based Encryption	<ul style="list-style-type: none"> ▪ Hashing ▪ Encryption 	SHA-2

Note: Unless otherwise indicated, all component servers are at Release 12c (12.1.3)

8.5 Troubleshooting FIPS 140 Issues

This section explains how to troubleshoot issues encountered with FIPS 140 configuration. It contains these topics:

- [FIPS 140 Troubleshooting for Stand-alone WebLogic Server](#)
- [FIPS 140 Troubleshooting for Oracle Platform Security Services](#)
- [FIPS 140 Troubleshooting for Oracle Web Services Manager](#)
- [FIPS 140 Troubleshooting for Database and JDBC Driver](#)

8.5.1 FIPS 140 Troubleshooting for Stand-alone WebLogic Server

Take the following steps to troubleshoot FIPS 140 mode for a stand-alone Oracle WebLogic Server:

During WebLogic Server Configuration

1. Make sure to prepend the server CLASSPATH with `jcmFIPS.jar` and `sslj.jar`.
2. To explicitly verify `*AES_256*` cipher suites, update the `local_policy.jar` and `US_export_policy.jar` in the `JAVA_HOME/jre/lib/security` directory with the corresponding file with unlimited strength.
3. Modify `JAVA_HOME/jre/lib/security/java.security` by putting `security.provider.1=com.rsa.jsafe.provider.JsafeJCE` and `security.provider.2=com.rsa.jsse.JsseProvider` on top of the list.

During Data Source Configuration

Make sure that the value of the DataSource property `oracle.net.ssl_version` is set to **1.0**.

Note: `oracle.net.ssl_version` is an optional Oracle WebLogic Server DataSource configuration property. A value of 1.0 represents connection through TLS v 1.0 Protocol.

8.5.2 FIPS 140 Troubleshooting for Oracle Platform Security Services

This section describes some troubleshooting tips in Oracle Platform Security Services (OPSS).

During WebLogic Domain Creation

You may see the following exceptions in `wlsconfig_XXXXX.log` during domain creation in FIPS 140 mode:

```
"CFGFWK-60455: The password
must be at least 8 alphanumeric characters with at least one number or
special character."

"Caused by: java.lang.NoSuchMethodError:
com.rsa.jsafe.JSAFE_SecretKey.generateInit([Ljava/security/SecureRandom;)"
```

This exception may occur if you are using cryptoJ 5 jars. Make sure you have installed Oracle WebLogic Server with cryptoJ 6 jars to avoid this error.

When Exporting from Domain Keystore

If you are using JKS and JCEKS type keystores in a FIPS 140-enabled domain, and see the following error:

```
Command FAILED, Reason:  
oracle.security.jps.service.keystore.KeyStoreServiceException: Failed to export  
the keystore
```

make sure that you have configured the following providers in the `java.security` file:

```
sun.security.provider.Sun  
com.sun.crypto.provider.SunJCE
```

8.5.3 FIPS 140 Troubleshooting for Oracle Web Services Manager

This section describes tips for issues originating in Oracle Web Services Manager.

During Message Protection Policy Enforcement

If you see this error during Oracle Web Services Manager message protection policy enforcement:

```
Caused by: java.lang.SecurityException: Algorithm not allowable in FIPS140 mode:  
MD5  
    at com.rsa.cryptoj.o.cc.b(Unknown Source)  
    at com.rsa.cryptoj.o.cc.f(Unknown Source)
```

make sure that certificates used in message protection enforcement are generated using FIPS 140-compliant algorithms like SHA1WithRSA or SHA256WithRSA.

If you encounter this error for the JKS keystore during message protection policy enforcement:

```
oracle.fabric.common.PolicyEnforcementException: WSM-00143 : Failure creating Java  
Keystore instance for type JKS.
```

make sure that `sun.security.provider.Sun` is configured in the JDK.

8.5.4 FIPS 140 Troubleshooting for Database and JDBC Driver

For complete details about security configuration for the database, the JDBC driver, including data source issues related to database, see the white paper "SSL With Oracle JDBC Thin Driver" on the Oracle Technology Network at:

<http://www.oracle.com/technetwork/middleware/id-mgmt/documentation/index.html>

Part IV

Deploying Applications

This part describes the deployment process and how to deploy applications to Oracle Fusion Middleware.

Part IV contains the following chapters:

- [Chapter 9, "Understanding the Deployment Process"](#)
- [Chapter 10, "Deploying Applications"](#)

Understanding the Deployment Process

Before you deploy Oracle Fusion Middleware applications, such as Java EE applications, you should understand the deployment process, such as designing and developing applications and deploying those applications to Managed Servers.

This chapter includes the following sections:

- [Section 9.1, "What Is a Deployer?"](#)
- [Section 9.2, "General Procedures for Moving from Application Design to Production Deployment"](#)
- [Section 9.3, "Diagnosing Typical Problems"](#)

9.1 What Is a Deployer?

A user in the role of **deployer** is responsible for deploying applications, such as Java EE applications, and ADF applications, to WebLogic Server instances or clusters.

A user who is functioning as a deployer should be granted the Oracle WebLogic Server deployer security role. The deployer security role allows deployment operations, as well as viewing the server configuration and changing startup and shutdown classes. To grant this role to a user, use the Oracle WebLogic Server Administration Console. See "Managing Security Roles" in the *Oracle WebLogic Server Administration Console Online Help* for more information.

9.2 General Procedures for Moving from Application Design to Production Deployment

This section describes the general procedures involved in moving from application design and development to deployment in a production environment. It contains the following topics:

- [Designing and Developing an Application](#)
- [Deploying an Application to Managed Servers](#)
- [Automating the Migration of an Application to Other Environments](#)

9.2.1 Designing and Developing an Application

In many cases, developers use Oracle JDeveloper to create their applications. Oracle JDeveloper is an integrated development environment (IDE) for building service-oriented applications using the latest industry standards for Java, XML, Web services, portlets, and SQL. JDeveloper supports the complete software development

life cycle, with integrated features for modeling, coding, debugging, testing, profiling, tuning, and deploying applications.

In this environment, you use the integrated Oracle WebLogic Server, which is packaged with Oracle JDeveloper for testing your applications.

For information about developing your applications, see:

- *Developing Applications for Oracle WebLogic Server*
- *Developing Fusion Web Applications with Oracle Application Development Framework*
- *Developing SOA Applications with Oracle SOA Suite*

9.2.2 Deploying an Application to Managed Servers

After you have designed and tested your application with the integrated Oracle WebLogic Server, you can deploy the application to a Managed Server instance. For example, you may have installed Oracle WebLogic Server and configured a domain, including a Managed Server, in your production environment and you want to deploy the application to that Managed Server.

The following books provide specific information about deploying the different types of applications:

- For Java EE applications, see *Deploying Applications to Oracle WebLogic Server*
- For Oracle ADF, see *Administering Oracle ADF Applications*
- For Oracle SOA Suite, see the *Developing SOA Applications with Oracle SOA Suite*

This section provides an outline of the major steps involved when you migrate your application from the integrated Oracle WebLogic Server to an environment separate from the development environment. Those general steps are:

1. Package the application:
 - For Java EE applications, you package the application in an EAR file. See "Preparing Applications and Modules for Deployment" in *Deploying Applications to Oracle WebLogic Server*.
 - For Oracle ADF, you package the application in an EAR file. See "What You May Need to Know About EAR Files and Packaging" in *Developing Fusion Web Applications with Oracle Application Development Framework*.
 - For Oracle SOA Suite, you package the application into a JAR or ZIP file. See "Understanding the Packaging Impact" in the *Developing SOA Applications with Oracle SOA Suite*.
2. Set up your environment. This includes:
 - Installing and configuring a domain and a Managed Server that is configured with the correct domain template. For example, if you are deploying an Oracle SOA Suite application, the Managed Server must use the Oracle SOA Suite domain template. The appropriate domain template is applied when you create the domain using the Configuration Wizard. Alternatively, you can extend a domain to use another domain template, as described in [Section 19.2](#).

For more information about installing and configuring for specific components, see:

- For Oracle ADF: "How to Install the ADF Runtime to the WebLogic Installation" in *Administering Oracle ADF Applications*

- For Oracle SOA Suite: "Installing Oracle SOA Suite and Oracle Business Process Management Suite", "Configuring the Oracle SOA Suite Domain" and "Configuring the Oracle Business Process Management Domain" in *Installing and Configuring Oracle SOA Suite and Business Process Management*
 - Creating any necessary schemas in an existing database. See *Creating Schemas with the Repository Creation Utility*.
 - Registering the MDS Repository with the Oracle WebLogic Server domain, if your application uses the MDS Repository. For example, Oracle SOA Suite applications require MDS. Some ADF applications involve customizations using MDS. See [Section 14.3.2.1.1](#) for information about registering the MDS Repository.
3. If your application uses a database, set up the JDBC data sources.
- For more information about setting up the JDBC data sources, see:
- For pure Java EE applications: *Administering JDBC Data Sources for Oracle WebLogic Server*
 - For Oracle ADF: "How to Create a JDBC Data Source for Oracle WebLogic Server" in *Administering Oracle ADF Applications*
 - For Oracle SOA Suite: "Creating Data Sources and Queues" in the *Developing SOA Applications with Oracle SOA Suite*
4. For Oracle SOA Suite, create connection factories and connection pooling. For more information, see "Creating Connection Factories and Connection Pooling" in the *Developing SOA Applications with Oracle SOA Suite*.
5. Create a connection to the target Managed Server.
- From Oracle JDeveloper, you can deploy your applications to Managed Server instances that reside outside JDeveloper. To do this, you must first create a connection to the server instance to which you want to deploy your application.
- For more information, see:
- For Oracle ADF: "How to Create a Connection to the Target Application Server" in *Developing Fusion Web Applications with Oracle Application Development Framework*
 - For Oracle SOA Suite: "Creating an Application Server Connection" in the *Developing SOA Applications with Oracle SOA Suite*
6. For Oracle SOA Suite, create a SOA-MDS connection, if the SOA composite application shares metadata with other composites. See "Creating a SOA-MDS Connection" in the *Developing SOA Applications with Oracle SOA Suite*.
7. Create a configuration plan or deployment plan, which contains information about environment-specific values, such as JDBC connection strings or host names of various servers. For more information, see:
- For pure Java EE applications: "Creating a New Deployment Plan to Configure an Application" in *Deploying Applications to Oracle WebLogic Server*
 - For Oracle SOA Suite: "Introduction to Configuration Plans" in the *Developing SOA Applications with Oracle SOA Suite*
8. Migrate application security, such as credentials, identities, and policies. For more information, see:
- For pure Java EE applications: "Migrating Security Data" in *Administering Security for Oracle WebLogic Server*

- For Oracle ADF: "Preparing the Secure Application for Deployment" in *Developing Fusion Web Applications with Oracle Application Development Framework*
 - For Oracle SOA Suite: "Enabling Security" in the *Developing SOA Applications with Oracle SOA Suite*
9. Create a deployment profile. A **deployment profile** packages or archives a custom ADF or SOA application and associated files so that the application can be deployed to a Managed Server instance. Deployment profiles are created at the project and application level.

For more information, see:

- For Oracle ADF: "How to Create Deployment Profiles" in *Developing Fusion Web Applications with Oracle Application Development Framework*
 - For Oracle SOA Suite: "Optionally Creating a Project Deployment Profile" in the *Developing SOA Applications with Oracle SOA Suite*
10. Migrate Oracle JDeveloper extensions for Oracle SOA Suite. [Table 9–1](#) shows the extensions and where they are documented:

Table 9–1 Oracle JDeveloper Extensions

Component	Extension	See:
Oracle SOA Suite	SOA extensions	"Enabling Oracle JDeveloper Extensions" in <i>Installing Oracle JDeveloper</i>

11. Deploy the application to a Managed Server.

For more information, see:

- For pure Java EE applications: "Exporting an Application for Deployment to New Environments" in *Deploying Applications to Oracle WebLogic Server*
- For Oracle ADF: "Deploying the Application" in *Developing Fusion Web Applications with Oracle Application Development Framework*
- For Oracle SOA Suite: "Deploying SOA Composite Applications" in *Developing SOA Applications with Oracle SOA Suite*

9.2.3 Automating the Migration of an Application to Other Environments

You can automate the migration of an application by using WLST or ant scripts. This makes it easier to deploy your application to multiple environments or Managed Servers and to deploy updated versions of the application.

For more information about using scripts to migrate an application to other environments, see:

- For pure Java EE applications: "Using the WebLogic Scripting Tool" in *Understanding the WebLogic Scripting Tool*
- For Oracle ADF: "Deploying Using Scripts and Ant" in *Administering Oracle ADF Applications*
- For Oracle SOA Suite: The following sections in the *Developing SOA Applications with Oracle SOA Suite*:
 - "Managing SOA Composite Applications with Scripts"

- "Managing SOA Composite Applications with ant Scripts"

9.3 Diagnosing Typical Problems

The following describes some of the typical problems that you may encounter when you deploy an application to a Managed Server:

- Connection information. Ensure that you have correctly configured the connection to the target Managed Server. See Steps 4, 5, and 6 in [Section 9.2.2](#).
- Oracle JDeveloper extensions. Ensure that you have migrated any Oracle JDeveloper extensions. See [Table 9-1](#).
- Data sources. Ensure that you have correctly configured JDBC data sources. See Step 3 in [Section 9.2.2](#).
- Security configuration. Ensure that you have migrated application security, such as credentials, identities, and policies. See Step 8 in [Section 9.2.2](#).

In addition, see the "Troubleshooting Common Deployment Errors" in the *Developing SOA Applications with Oracle SOA Suite* for information about troubleshooting SOA applications.

Deploying Applications

Deployment is the process of packaging application files as an archive file and transferring them to a target application server. This chapter describes how to deploy, redeploy, and undeploy applications to Oracle Fusion Middleware.

It contains the following sections:

- [Section 10.1, "Overview of Deploying Applications"](#)
- [Section 10.2, "Understanding and Managing Data Sources"](#)
- [Section 10.3, "Deploying, Undeploying, and Redeploying Java EE Applications"](#)
- [Section 10.4, "Deploying, Undeploying, and Redeploying Oracle ADF Applications"](#)
- [Section 10.5, "Deploying, Undeploying, and Redeploying SOA Composite Applications"](#)
- [Section 10.6, "Managing Deployment Plans"](#)
- [Section 10.7, "About the Common Deployment Tasks in Fusion Middleware Control"](#)
- [Section 10.8, "Changing MDS Configuration Attributes for Deployed Applications"](#)

10.1 Overview of Deploying Applications

Oracle WebLogic Server provides a Java EE-compliant infrastructure for deploying, undeploying, and redeploying Java EE-compliant applications and modules.

The following topics describe:

- [What Types of Applications Can You Deploy?](#)
- [Understanding Deployment, Redeployment, and Undeployment](#)

10.1.1 What Types of Applications Can You Deploy?

You can deploy the following into Oracle WebLogic Server:

- A complete Java EE application packaged as an Enterprise Archive (EAR) file.
- Standalone modules packaged as Java Archive files (JARs) containing Web services, Enterprise JavaBeans (EJBs), application clients (CARs), or resource adapters (RARs).
- An ADF application. Oracle Application Development Framework (Oracle ADF) is an end-to-end application framework that builds on Java Platform, Enterprise

Edition (Java EE) standards, and open-source technologies to simplify and accelerate implementing service-oriented applications.

- An Oracle SOA Suite composite application. A SOA composite application is a single unit of deployment that greatly simplifies the management and lifecycle of SOA applications.

A Metadata Archive (MAR) is a compressed archive of selected metadata, such as the application-level deployment profile, for an application. A MAR is used to deploy metadata content to the metadata service (MDS) repository. ADF applications and SOA composite applications use a MAR as a container for content that is deployed to the MDS Repository.

Note: If your application uses password indirection in the application-level data source, you cannot use Fusion Middleware Control to deploy the application. The section "Deploying an Application to an EAR File to run on Oracle WebLogic Server" in the Oracle JDeveloper Help describes how to change the settings of the application to be able to deploy the application using Fusion Middleware Control.

You can use Fusion Middleware Control, Oracle WebLogic Server Administration Console, Oracle JDeveloper, or the command line to deploy, undeploy, or redeploy an application. Which method you use depends on the type of application, as described in [Table 10-1](#).

Table 10-1 Tools to Deploy Applications

Type of Application	Tools to Use
Pure Java EE application	Oracle WebLogic Server Administration Console Fusion Middleware Control: Deployment Wizard Oracle JDeveloper WLST command line
ADF application	Fusion Middleware Control: Deployment Wizard Oracle JDeveloper WLST command line
SOA Composite application	Fusion Middleware Control: SOA Composite Deployment Wizard Oracle JDeveloper WLST command line

If your application uses an MDS Repository, you must register the repository with the Oracle WebLogic Server domain before you deploy your application. Applications such as custom Java EE applications developed by your organization and some Oracle Fusion Middleware component applications, such as Oracle B2B and Oracle Web Services Manager, use an MDS Repository. For information about the MDS Repository and registering the repository, see [Section 14.3](#).

Note: If your application contains an application-level credential store, and you are moving the application from a test to a production environment, you must reassociate the credential store, as described in "Reassociating the Domain Policy Store" in *Securing Applications with Oracle Platform Security Services*.

10.1.2 Understanding Deployment, Redeployment, and Undeployment

When you deploy an application, you deploy it to the application server for the first time.

When you redeploy an application, you can:

- Redeploy a new version of the application; the previous version is still available, but the state is set to "Retired."

This is known as the production redeployment strategy. Oracle WebLogic Server automatically manages client connections so that only new client requests are directed to the new version. Clients already connected to the application during the redeployment continue to use the older version of the application until they complete their work, at which point Oracle WebLogic Server automatically retires the older application.

- Redeploy the same version of the application or redeploy an application that is not assigned a version; the application version you select is replaced with the new deployment.
- Redeploy a previous version of the application; the earlier, retired version is set to "Active" and the later version is set to "Retired."

When you undeploy an application, Oracle WebLogic Server stops the application and removes staged files from target servers. It does not remove the original source files used for deployment.

10.2 Understanding and Managing Data Sources

The following topics describe data sources and how to manage them:

- [Understanding Data Sources](#)
- [Creating and Managing JDBC Data Sources](#)

10.2.1 Understanding Data Sources

A **data source** is a Java object that application components use to obtain connections to a relational database. Specific connection information, such as the URL or user name and password, are set on a data source object as properties and do not need to be explicitly defined in an application's code. This abstraction allows applications to be built in a portable manner, because the application is not tied to a specific back-end database. The database can change without affecting the application code.

Applications use the Java Naming and Directory Interface (JNDI) API to access a data source object. The application uses a JNDI name that is bound to the data source object. The JNDI name is logical and can be mapped to any data source object. Like data source properties, using JNDI provides a level of abstraction, since the underlying data source object can change without any changes required in the application code. The end result is the details of accessing a database are transparent to the application.

See *Administering JDBC Data Sources for Oracle WebLogic Server* for more information about data sources.

When you configure certain Oracle Fusion Middleware components, such as Oracle SOA Suite, using the Oracle WebLogic Server Configuration Wizard, you specify the data source connection information. If the components use the MDS Repository, the Configuration Wizard prepends `mds-` to the data source name to indicate that the data source is a system data source used by MDS Repository.

See *Creating WebLogic Domains Using the Configuration Wizard* for information about specifying data sources with the Configuration Wizard.

If you are using Oracle Real Application Clusters (Oracle RAC) or Oracle Fusion Middleware Cold Failover Cluster, you must configure one of the following types of data sources:

- **Multi data sources**

To use multi data sources, you must use the Oracle WebLogic Server Administration Console. Note that if you create a multi data source and you add an existing MDS data source to it, the data source you added is no longer considered a valid MDS Repository. The repository is not displayed in Fusion Middleware Control or Oracle WebLogic Server Administration Console. For example, the MDS Repository is not listed in the Fusion Middleware Control navigation pane and is not displayed as a choice for a target metadata repository when you deploy an application.

- **GridLink data sources**

To use GridLink data sources, you can use the Oracle WebLogic Server Administration Console or Fusion Middleware Control, as described in [Section 10.2.2.5](#).

See *Administering JDBC Data Sources for Oracle WebLogic Server* for more information about configuring multi data sources and GridLink data sources

10.2.2 Creating and Managing JDBC Data Sources

You can create and manage JDBC data sources using the following management tools:

- The Oracle WebLogic Server Administration Console
- The WebLogic Scripting Tool (WLST)
- Fusion Middleware Control

To create an MDS data source manually, you should use Fusion Middleware Control or WLST to set the correct attributes for the data source. The MDS data source is displayed in the navigation pane in Fusion Middleware Control and in the domain structure in the Administration Console. If your application uses an MDS Repository, you must register the repository with the Oracle WebLogic Server domain before you deploy your application. For information about the MDS Repository and registering the repository, see [Section 14.3](#).

Note: When you create the data source, you must use the MDS schema created by the Repository Creation Utility (RCU), not other schemas.

Although it is not recommended, you can also use the Oracle WebLogic Server Administration Console to create a MDS data source. If you do, note the following:

- You must prefix the data source name with `mds-` if you intend it to be used with MDS Repository.
- You must target the data source to the Administration Server and to all Managed Servers to which you are deploying applications that need the data source.
- You must turn off global transactions.

See *Administering JDBC Data Sources for Oracle WebLogic Server* for information about creating and managing a data source using the Oracle WebLogic Server Administration Console or WLST and for more information about configuring multiple data sources.

The following topics describe how to create and manage JDBC data sources with Fusion Middleware Control:

- [Creating a JDBC Data Source Using Fusion Middleware Control](#)
- [Editing a JDBC Data Source Using Fusion Middleware Control](#)
- [Monitoring a JDBC Data Source Using Fusion Middleware Control](#)
- [Controlling a JDBC Data Source Using Fusion Middleware Control](#)
- [Creating a GridLink Data Source Using Fusion Middleware Control](#)

10.2.2.1 Creating a JDBC Data Source Using Fusion Middleware Control

To create a JDBC data source using Fusion Middleware Control:

1. From the **WebLogic Domain** menu, choose **JDBC Data Sources**.

The JDBC Data Sources page is displayed, as shown in the following figure:

The screenshot shows the Fusion Middleware Control interface for 'JDBC Data Sources'. At the top, it indicates the user is logged in as 'weblogic' and the page was refreshed on Jan 28, 2014 at 11:29:59 AM PST. The breadcrumb path is '/Domain_base_domain/base_domain > JDBC Data Sources'. Below the title, a message states: 'This page lists the JDBC system data sources that have been created in this domain. You can create or delete the system data sources from this page.' A toolbar contains buttons for 'View', 'Create', 'Create Like', 'Delete', and 'Detach'. The main content is a table with the following data:

Name	JNDI Name	Type	Targets
BamDataSource	jdbc/BeamDataSource	Generic	bam_server1
BamJobSchedDataSource	jdbc/BeamJobScheduler	Generic	bam_server1
EDNDataSource	jdbc/EDNDataSource	Generic	soa_cluster_1
EDNLocalTxDataSource	jdbc/EDNLocalTxDataSource	Generic	soa_cluster_1
LocalSvcTblDataSource	jdbc/LocalSvcTblDataSource	Generic	AdminServer

2. From **Create**, select **Generic Data Source**.
3. Follow the instructions in the wizard to set the properties of the data source and to target the data source for one or more of the Managed Servers in the domain.

For help on individual fields and properties, use your mouse to give focus to a field. Fusion Middleware Control displays a popup definition of the field.

Note that the data source properties you define in Fusion Middleware Control are similar to those you define when creating data sources in the Oracle WebLogic Server Administration Console. As a result, you can also refer to "Creating a JDBC Data Source" in *Administering JDBC Data Sources for Oracle WebLogic Server* for more information about the data source properties.

10.2.2.2 Editing a JDBC Data Source Using Fusion Middleware Control

To edit an existing JDBC data source using Fusion Middleware Control:

1. From the **WebLogic Domain** menu, choose **JDBC Data Sources**.
The JDBC Data Sources page is displayed.
2. Click the data source that you want to edit.
The page for that particular JDBC Data Source is displayed.
3. Use the tabs on this page to modify the properties of the selected data source.

For help on individual fields and properties, use your mouse to give focus to a field. Fusion Middleware Control displays a popup definition of the field.

Note that the data source properties you edit in Fusion Middleware Control are similar to those you edit when editing data sources in the Oracle WebLogic Server Administration Console. As a result, you can also refer to "Creating a JDBC Data Source" in *Administering JDBC Data Sources for Oracle WebLogic Server* for more information about the data source properties.

10.2.2.3 Monitoring a JDBC Data Source Using Fusion Middleware Control

To monitor a JDBC data source using Fusion Middleware Control:

1. From the **WebLogic Domain** menu, choose **JDBC Data Sources**.
The JDBC Data Sources page is displayed.
2. Select the data source that you want to monitor.
3. Click **Monitoring** to display the Monitor JDBC Data Source page.
This page shows the current instances of the selected data source.

Note that only data sources that are targeted to a running Managed Server are shown on this page. If a specific data source is not listed on the monitoring page, then edit the data source to be sure it is targeted to a running Managed Server.

4. For each data source instance, review the performance metrics.

10.2.2.4 Controlling a JDBC Data Source Using Fusion Middleware Control

To start, stop, suspend, resume, or clear the statement cache for a JDBC data source using Fusion Middleware Control:

1. From the **WebLogic Domain** menu, choose **JDBC Data Sources**.
The JDBC Data Sources page is displayed.
2. Select the data source that you want to edit.
3. Select the Control tab.

Note that only data sources that are targeted to a running Managed Server are shown on this page. If a specific data source is not listed on the control page, edit the data source to be sure that it is targeted to a running Managed Server.

4. Select the instance and click Start, Stop, Resume, Suspend, Shrink, Reset, Clear Statement Cache to control or change the state of the selected JDBC data source.

Note that the commands you select on this page are similar to those available when you are managing data sources in the Oracle WebLogic Server Administration Console. Refer to "Managing WebLogic JDBC Resources" in

Administering JDBC Data Sources for Oracle WebLogic Server for more information about the JDBC data source control options.

10.2.2.5 Creating a GridLink Data Source Using Fusion Middleware Control

A single GridLink data source provides connectivity between WebLogic Server and an Oracle Database service targeted to an Oracle RAC cluster. For detailed information about GridLink data sources, see "Creating a GridLink Data Source" in *Administering JDBC Data Sources for Oracle WebLogic Server*.

To create a Grid Link data source using Fusion Middleware Control:

1. From the **WebLogic Domain** menu, choose **JDBC Data Sources**.

The JDBC Data Sources page is displayed.

2. From **Create**, select **GridLink Data Source**.

3. Follow the instructions in the wizard to set the properties of the data source and to target the data source for one or more of the Managed Servers in the domain.

For help on individual fields and properties, use your mouse to give focus to a field. Fusion Middleware Control displays a popup definition of the field.

Note that the data source properties you define in Fusion Middleware Control are similar to those you define when creating data sources in the Oracle WebLogic Server Administration Console. As a result, you can also refer to "Creating a GridLink Data Source" in *Administering JDBC Data Sources for Oracle WebLogic Server* for more information about the data source properties.

10.3 Deploying, Undeploying, and Redeploying Java EE Applications

You can use Fusion Middleware Control, Oracle WebLogic Server Administration Console, Oracle JDeveloper, or the command line to deploy, undeploy, or redeploy a Java EE application. The following topics describe using Fusion Middleware Control and the command line to accomplish these tasks:

- [Deploying Java EE Applications](#)
- [Undeploying Java EE Applications](#)
- [Redeploying Java EE Applications](#)

See *Deploying Applications to Oracle WebLogic Server* for information about deploying using Oracle WebLogic Server Administration Console and the WLST command line.

10.3.1 Deploying Java EE Applications

You can deploy an application to a Managed Server instance or a cluster. This section describes how to deploy an application to a Managed Server. It contains the following topics:

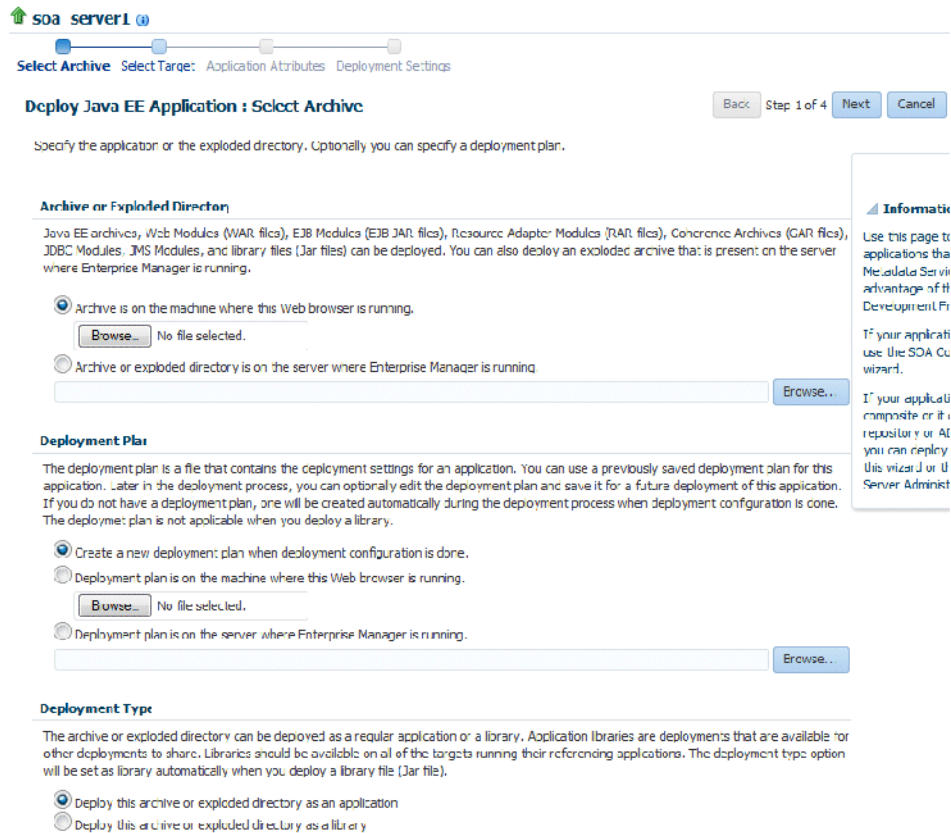
- [Deploying Java EE Applications Using Fusion Middleware Control](#)
- [Deploying Java EE Applications Using WLST](#)

10.3.1.1 Deploying Java EE Applications Using Fusion Middleware Control

To deploy a Java EE application to a Managed Server using Fusion Middleware Control:

1. From the navigation pane, expand the domain.

2. Select the server in which you want to deploy the application.
The server home page is displayed.
3. From the WebLogic Server menu, choose **Control**, then **Deployments**.
The Deployments page is displayed.
4. Click **Deploy** to open the Deploy Java EE Application Assistant.
The Select Archive page is displayed, as shown in the following figure:



5. In the Archive or Exploded Directory section, you can select one of the following:
 - **Archive is on the machine where this browser is running.** Enter the location of the archive or click **Browse** to find the archive file.
 - **Archive or exploded directory is on the server where Enterprise Manager is running.** Enter the location of the archive or click **Browse** to find the archive file.
6. In the Deployment Plan section, you can select one of the following:
 - **Create a new deployment plan when deployment configuration is done.**
 - **Deployment plan is on the machine where this Web browser is running.** If you select this option, enter the path to the plan.
 - **Deployment plan is on the server where Enterprise Manager is running.** If you select this option, enter the path to the plan.
7. In the Deployment Type section, you can select one of the following:
 - **Deploy this archive or exploded directory as an application**

- **Deploy this archive or exploded directory as a library**
8. Click **Next**.

The Select Target page is displayed.
 9. Select the target to which you want to deploy the application. The Administration Server, Managed Servers, and clusters are listed. You can select a cluster, one or more Managed Servers in the cluster, or a Managed Server that is not in a cluster. Although the Administration Server is shown in the list of targets, you should not deploy an application to it. The Administration Server is intended only for administrative applications such as the Oracle WebLogic Server Administration Console.
 10. Click **Next**.

The Application Attributes page is displayed.
 11. In the Application Attributes section, for **Application Name**, enter the application name.
 12. In the Context Root of Web Modules section, if the Web module does not have the context root configured in the application.xml file, you can specify the context root for your application. The **context root** is the URI for the Web module. Each Web module or EJB module that contains Web services may have a context root.
 13. In the Distribution section, you can select one of the following:
 - **Install and start application (servicing all requests)**
 - **Install and start application in administration mode (servicing only admin requests)**
 - **Install only. Do not start**
 14. You can expand Other Options, which provides the following for Application Source Accessibility:
 - Use the defaults defined by the deployment's targets. Recommended selection.
 - Copy this application onto every target. During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted.
 - Make the application accessible from the source location that it will be deployed on. You must ensure that each target can reach the location.
 15. In Other Options, you can also select one of the following for Deployment Plan Source Accessibility:
 - Use the same accessibility as the application.
 - Copy the deployment plan onto every target. During deployment, the files will be copied automatically to the Managed Servers to which the application is targeted.
 - Make the deployment plan accessible from the source location that it will be deployed on. You must ensure that each target can reach the location.
 16. Click **Next**.

The Deployment Wizard, Deployment Settings page is displayed.
 17. On this page, you can perform common tasks before deploying your application or you can edit the deployment plan or save it to a disk.

See [Section 10.7](#) for more detailed information about these tasks.

Depending on the type of application, in the Deployment Tasks section, you can:

- **Configure Web modules:** Click **Go to Task** in the Configure Web Modules row. The Configure Web Modules page is displayed. Click **Configure General Properties** to view and edit the general configuration for the Web Module or **Map Resource References** to map the resource references.

For example, you can change the session invalidation interval or the maximum age of session cookies.

- **Configure EJB modules:** Click **Go to Task** in the Configure EJB modules row to set standard EJB deployment descriptor properties. The Configure EJB Modules page is displayed. Click **Configure EJB Properties** to view and edit the general configuration for the EJBs or **Map Resource References** to map the resource preferences.

For example, you can configure the maximum number of beans in the free pool or the network access point.

- **Configure application security:** Click **Go to Task** in the Configure Application Security row. Depending on what type of security is used, different pages are displayed, as described in [Section 10.7](#).
- **Configure persistence:** Click **Go to Task** in the Configure Persistence row to configure Java Persistent API (JPA) persistence units.

18. Expand **Deployment Plan**.

You can edit and save the deployment plan, if you choose. If you edit the deployment plan and change descriptor values, those changes are saved to the deployment plan. In addition, the following configurations are saved to the deployment plan:

- Application attributes
- Web module configuration
- EJB configuration

Application attributes related to MDS are stored in the file `adf-config.xml`. Application security attributes are stored in `weblogic-application.xml`.

Fusion Middleware Control updates the relevant files and repackages the `.ear` file.

19. Click **Deploy**.

Fusion Middleware Control displays processing messages.

20. When the deployment is completed, click **Close**.

To deploy an application to multiple servers at the same time, navigate to the domain. Then, from the WebLogic Domain menu, select **Application Deployment**, then **Deploy**. The deployment wizard displays a page where you can select the servers.

To deploy an application to a cluster, select the cluster. Then, from the Cluster menu, select **Application Deployment**, then **Deploy**.

10.3.1.2 Deploying Java EE Applications Using WLST

You can deploy an application using the WLST command line. To deploy a Java EE application when WLST is connected to the Administration Server, you use the WLST command `deploy`, using the following format:

```
deploy(app_name, path [,targets] [,stageMode] [,planPath] [,options])
```

You must invoke the deploy command on the computer that hosts the Administration Server.

For example, to deploy the application mainWebApp:

```
deploy("myApp", "/scratch/applications/wlserver/samples/server/examples/build/mainWebApp")
```

You can also deploy the application using the weblogic.deployer, as shown in the following example:

```
java weblogic.Deployer -adminurl http://localhost:7001
  -user username -password password -deploy
  -name myApp c:\localfiles\mainWebApp
  -plan c:\localfiles\productionEnvPlan.xml
```

See Also:

- "Deployment Tools" in *Deploying Applications to Oracle WebLogic Server* for more information about using WLST to deploy applications
- *WLST Command Reference for WebLogic Server*

10.3.2 Undeploying Java EE Applications

You can undeploy an application or a specific version of an application from a Managed Server instance or a cluster. This section describes how to undeploy an application from a Managed Server. If an application has been deployed to multiple servers, when you undeploy it using Fusion Middleware Control, the application is undeployed from all the servers.

This section contains the following topics:

- [Undeploying Java EE Applications Using Fusion Middleware Control](#)
- [Undeploying Java EE Applications Using WLST](#)

10.3.2.1 Undeploying Java EE Applications Using Fusion Middleware Control

To undeploy a Java EE application from a Managed Server using Fusion Middleware Control:

1. From the navigation pane, expand **Application Deployments**.
2. Select the application to undeploy.
The application home page is displayed.
3. From the Domain Application Deployment menu, choose **Deployments**.
4. Select the application.
5. In Confirmation page, click **Undeploy**.
Processing messages are displayed.
6. When the operation completes, click **Close**.

Alternatively, you can navigate to the domain, Managed Server, or cluster. Then, from the target's menu, choose **Application Deployment**, then **Undeploy**. In the Select Application page, select the application you want to undeploy.

10.3.2.2 Undeploying Java EE Applications Using WLST

You can undeploy an application using the WLST command line. To undeploy a Java EE application when WLST is connected to the Administration Server, you use the WLST command `undeploy`, using the following format:

```
undeploy(app_name, path [, targets] [, options])
```

You must invoke the undeploy command on the computer that hosts the Administration Server.

For example, to undeploy the application `businessApp` from all target servers and specify that WLST wait 60,000 ms for the process to complete:

```
wls:/mydomain/serverConfig> undeploy('businessApp', timeout=60000)
```

10.3.3 Redeploying Java EE Applications

You can redeploy a new version of an updated application, redeploy the same version, or redeploy a non-versioned application. You can redeploy an application to a cluster or a Managed Server.

The following sections describe how to redeploy an application to a Managed Server:

- [Redeploying Java EE Applications Using Fusion Middleware Control](#)
- [Redeploying Java EE Applications Using WLST](#)

If you are redeploying a non-versioned application or a versioned application with the same version, note the following:

- The file name and path for the archive you are redeploying must be identical to the file name and path you used when you initially deployed the application.
For example, if the file name and path of the original application was `/dua0/staging/myApp.ear`, then the revised application must be `/dua0/staging/myApp.ear`.
- If you initially deployed the application using the Oracle WebLogic Server Administration Console or WLST or other management tools other than Fusion Middleware Control, then you cannot redeploy the application using Fusion Middleware Control.

10.3.3.1 Redeploying Java EE Applications Using Fusion Middleware Control

To redeploy a Java EE application to a Managed Server using Fusion Middleware Control:

1. From the navigation pane, expand **Application Deployments**.
2. Select the application to redeploy.
The application home page is displayed.
3. From the Application Deployment menu, choose **Deployments**.
4. Click **Redeploy**.
The Select Application page is displayed.
5. Click **Next**.
6. In the Archive or Exploded Directory section, you can select one of the following:
 - **Use the archive or exploded directory in the existing source location of the application on the Administration Server.**

- **Archive is on the machine where this browser is running.** Enter the location of the archive or click **Browse** to find the archive file.
 - **Archive or exploded directory is on the server where Enterprise Manager is running.** Enter the location of the archive or click **Browse** to find the archive file.
7. In the Deployment Plan section, you can select one of the following:
- **Create a new deployment plan when deployment configuration is done.**
 - **Deployment plan is on the machine where this Web browser is running.** Enter the path to the plan or click **Browse** to find the plan file.
 - **Deployment plan is on the server where Enterprise Manager is running.** Enter the path to the plan or click **Browse** to find the plan file.
8. Click **Next**.
- The Application Attributes page is displayed.
9. Click **Next**.
- The Deployment Wizard, Deployment Settings page is displayed.
10. On this page, you can perform common tasks before deploying your application or you can edit the deployment plan or save it to a disk. Depending on the type of application, in the Deployment Tasks section, you can:
- Configure Web modules
 - Configure application security
 - Configure EJB modules
 - Configure persistence
- See [Section 10.7](#) for detailed information about these tasks.
11. Expand **Deployment Plan**.
- You can edit and save the deployment plan, if you choose. If you edit the deployment plan and change descriptor values, those changes are saved to the deployment plan. In addition, the following configurations are saved to the deployment plan:
- Application attributes
 - Web module configuration
 - EJB configuration
- Application attributes related to MDS are stored in the file `adf-config.xml`.
Application security attributes are stored in `weblogic-application.xml`.
- Fusion Middleware Control updates the relevant files and repackages the `.ear` file.
12. Click **Redeploy**.
- Processing messages are displayed.
13. When the operation completes, click **Close**.
- To redeploy an application to a cluster, select the cluster. Then, from the target's menu, select **Application Deployment**, then **Redeploy**.

10.3.3.2 Redeploying Java EE Applications Using WLST

You can redeploy an application using the WLST command line. To redeploy a Java EE application when WLST is connected to the Administration Server, you use the WLST command `redeploy`, using the following format:

```
redeploy(app_name [,planpath] [,options])
```

You must invoke the redeploy command on the computer that hosts the Administration Server.

For example, to redeploy the application `businessApp` from all target servers:

```
redeploy('businessApp')
```

10.4 Deploying, Undeploying, and Redeploying Oracle ADF Applications

Oracle ADF is an end-to-end application framework that builds on Java Platform, Enterprise Edition (Java EE) standards and open-source technologies to simplify and accelerate implementing service-oriented applications.

You can use Fusion Middleware Control, Oracle WebLogic Server Administration Console, Oracle JDeveloper, or the command line to deploy, undeploy, or redeploy an Oracle ADF application. The following topics describe using Fusion Middleware Control, the Administration Console, and the command line to accomplish these tasks:

- [Deploying Oracle ADF Applications](#)
- [Undeploying Oracle ADF Applications](#)
- [Redeploying Oracle ADF Applications](#)

See *Developing Fusion Web Applications with Oracle Application Development Framework* for information on developing ADF applications and for deploying them using Oracle JDeveloper

10.4.1 Deploying Oracle ADF Applications

You can deploy an application to a WebLogic Server Managed Server instance or a cluster. This section describes how to deploy an application to a Managed Server and assumes that you have created an `.ear` file containing the ADF application.

This section contains the following topics:

- [Deploying ADF Applications Using Fusion Middleware Control](#)
- [Deploying ADF Applications Using WLST](#)
- [Deploying ADF Applications Using the Administration Console](#)

10.4.1.1 Deploying ADF Applications Using Fusion Middleware Control

To deploy an Oracle ADF application using Fusion Middleware Control:

1. From the navigation pane, expand the domain.
2. Select the server in which you want to deploy the application.
The server home page is displayed.
3. From the WebLogic Server menu, choose **Control**, then **Deployments**.
The Deployments page is displayed.
4. Click **Deploy**.

The Select Archive page is displayed.

5. In the Archive or Exploded Directory section, you can select one of the following:
 - **Archive is on the machine where this browser is running.** Enter the location of the archive or click **Browse** to find the archive file.
 - **Archive or exploded directory is on the server where Enterprise Manager is running.** Enter the location of the archive or click **Browse** to find the archive file.
6. In the Deployment Plan section, you can select one of the following:
 - **Create a new deployment plan when deployment configuration is done.**
 - **Deployment plan is on the machine where this Web browser is running.** Enter the path to the plan.
 - **Deployment plan is on the server where Enterprise Manager is running.** Enter the path to the plan.
7. In the Deployment Type section, you can select one of the following:
 - **Deploy this archive or exploded directory as an application**
 - **Deploy this archive or exploded directory as a library**
8. Click **Next**.

The Select Target page is displayed.

9. Select the target to which you want to deploy the application. The Administration Server, Managed Servers, and clusters are listed. You can select a cluster, one or more Managed Servers in the cluster, or a Managed Server that is not in a cluster. Although the Administration Server is shown in the list of targets, you should not deploy an application to it. The Administration Server is intended only for administrative applications such as the Oracle WebLogic Server Administration Console.
10. Click **Next**.

The Application Attributes page is displayed, as shown in the following figure:

soa_server1

Select Archive Select Target **Application Attributes** Deployment Settings

Deploy Java EE Application : Application Attributes Back Step 3 of 4 Next Deploy Cancel

Archive Type Java EE Application (EAR file)
 Deployment Plan Create a new plan
 Deployment Target soa_server1
 Deployment Type Application

* Application Name

Context Root of Web Modules

Web Module	Context Root
mdsappdbweb.war	mdsappdbweb

Target Metadata Repository

Select the metadata repository and specify the partition in the repository that the application will be deployed to.

Information
 The metadata repository "mds-appDBRepos (Database)" specified in this application is not a registered repository in this domain. Select a registered repository.

* Repository Name
 Repository Type Database
 * Partition

Distribution

Install and start application (servicing all requests)
 Install and start application in administration mode (servicing only administration requests)
 Install only. Do not start.

11. In the Application Attributes section, for **Application Name**, enter the application name.
12. In the Context Root of Web Modules section, if the Web module does not have the context root configured in the application.xml file, you can specify the context root for your application. The context root is the URI for the Web module. Each Web module or EJB module that contains Web services may have a context root.
13. In the Target Metadata Repository section, you can choose the repository and partition for this application. If the partition name is not specified in the adf-config.xml file, the application name plus the version is used as the default partition name. This ensures that the partition used is unique in the domain so that the metadata for different applications are not accidentally imported into the same repository partition and overwrite each other. Typically, each application's metadata is deployed to its own partition.
 - To change the repository, click the icon next to the **Repository Name**. In the Metadata Repositories dialog box, select the repository and click **OK**.
 - To change the partition, enter the partition name in **Partition Name**. Oracle recommends that you create a new partition for each application. If you enter a name of a partition that does not exist, the partition is created.

The adf-config.xml file in the .ear file is updated with the new information.

If the partition or repository specified in the application is not valid in the domain, Fusion Middleware Control displays a message.

14. If the application's adf-config.xml file archive contains MDS configuration for an MDS shared repository, the Shared Metadata Repository section is displayed. In this section, you can choose the repository and partition for this application. If the partition or repository specified in the application is not valid in the domain, Fusion Middleware Control displays a message.

If you change the repository or partition, the `adf-config.xml` file in the `.ear` file is updated with the new information.

15. In the Distribution section, you can select one of the following:

- **Install and start application (servicing all requests)**
- **Install and start application in admin mode (servicing only administration requests)**
- **Install only. Do not start.**

16. You can expand Other Options. See [Section 10.3.1](#) for a description of those options.

17. Click **Next**.

The Deployment Wizard, Deployment Settings page is displayed.

18. On this page, you can perform common tasks before deploying your application or you can edit the deployment plan or save it to a disk. Depending on the type of application, in the Deployment Tasks section, you can:

- **Configure Web modules:** Click **Go to Task** in the Configure Web Modules row. The Configure Web Modules page is displayed. Click **Configure General Properties** to view and edit the general configuration for the Web Module or **Map Resource References** to map the resource references.

For example, you can change the session invalidation interval or the maximum age of session cookies.

- **Configure EJB modules:** Click **Go to Task** in the Configure EJB modules row to set standard EJB deployment descriptor properties. The Configure EJB Modules page is displayed. Click **Configure EJB Properties** to view and edit the general configuration for the EJBs or **Map Resource References** to map the resource preferences.

For example, you can configure the maximum number of beans in the free pool or the network access point.

- **Configure application security:** Click **Go to Task** in the Configure Application Security row. Depending on what type of security is used, different pages are displayed, as described in [Section 10.7](#).
- **Configure persistence:** Click **Go to Task** in the Configure Persistence row to configure Java Persistent API (JPA) persistence units.
- **Configure ADF Connections:** To modify the ADF connections, click **Go to Task** in the Configure ADF Connections row. The Configure ADF Connections page is displayed, showing the current connection information. To modify a connection type, click the **Edit** icon for a particular row. For example, you can modify the connection information for an external application. For more information about ADF connections, see *Developing Fusion Web Applications with Oracle Application Development Framework*.

For more information about these options, see [Section 10.7](#).

19. Expand **Deployment Plan**.

You can edit and save the deployment plan, if you choose.

20. Click **Deploy**.

Fusion Middleware Control displays processing messages.

21. When the deployment is completed, click **Close**.

10.4.1.2 Deploying ADF Applications Using WLST

To deploy an ADF application using the WLST command line:

1. If your application uses an MDS Repository, you must configure the application archive (.ear) file before you deploy your application. You must provide the repository information for the deploy target repository and any shared metadata repositories using the WLST `getMDSArchiveConfig` command. The repository specified must already be registered with the domain before deploying the application. The following example show how to use this command to get the `MDSArchiveConfig` and call the `setAppMetadataRepository` method to set the deploy target repository. Otherwise, your application will fail to start.

```
wls:/offline> archive = getMDSArchiveConfig(fromLocation='/tmp/App1.ear')
wls:/offline> archive.setAppMetadataRepository(repository='AppRepos1',
partition='partition1', type='DB', jndi='mds-jndi1')
```

The operation places the changes in the MDS configuration portion of the `adf-config.xml` file in the archive file.

2. Save the changes to the original .ear file, using the following command:

```
wls:/offline> archive.save()
```

3. Deploy the application.

To deploy an application when WLST is connected to the Administration Server, you use the WLST command `deploy`, using the following format:

```
deploy(app_name, path [,targets] [,stageMode] [,planPath] [,options])
```

You must invoke the `deploy` command on the computer that hosts the Administration Server.

For example, to deploy the application `myApp`:

```
deploy("myApp", "/scratch/applications/myApp", targets='myserver',
timeout=120000)
```

See Also:

- "Deployment Tools" in *Deploying Applications to Oracle WebLogic Server* for more information about using WLST to deploy applications
- *WLST Command Reference for WebLogic Server*

10.4.1.3 Deploying ADF Applications Using the Administration Console

To deploy the application using the Oracle WebLogic Server Administration Console:

1. If you have not already done so, in the Change Center of the Administration Console, click **Lock & Edit**.
2. In the left pane of the Administration Console, select **Deployments**.
3. In the right pane, click **Install**.

10.4.2 Undeploying Oracle ADF Applications

To undeploy an Oracle ADF application using Fusion Middleware Control:

1. From the navigation pane, expand **Application Deployments**.
2. Select the application to undeploy.

The application home page is displayed.

3. From the Domain Application Deployment menu, choose **Deployments**.
4. Select the application.
5. In Confirmation page, click **Undeploy**.

Processing messages are displayed.

6. When the operation completes, click **Close**.

Alternatively, you can navigate to the domain, Managed Server, or cluster. Then, from the target's menu, choose **Application Deployment**, then **Undeploy**. In the Select Application page, select the application you want to undeploy.

Note that when you undeploy an application, documents stored in the MDS partition are not deleted.

10.4.3 Redeploying Oracle ADF Applications

When you redeploy an application, if the application contains a Metadata Archive (MAR), the contents of the MAR is imported to the application's metadata repository only if the MAR is changed. If the MAR is unchanged from previous deployment of the application, it is ignored.

If you are redeploying a non-versioned application or a versioned application with the same version, note the following:

- The file name and path for the archive you are redeploying must be identical to the file name and path you used when you initially deployed the application.

For example, if the file name and path of the original application was /dua0/staging/myApp.ear, then the revised application must be /dua0/staging/myApp.ear.

- If you initially deployed the application using the Oracle WebLogic Server Administration Console or WLST or other management tools other than Fusion Middleware Control, then you cannot redeploy the application using Fusion Middleware Control.

To redeploy an Oracle ADF application using Fusion Middleware Control:

1. From the navigation pane, expand **Application Deployments**.

2. Select the application to redeploy.

The application home page is displayed.

3. From the Domain Application Deployment menu, choose **Deployments**.

4. Click **Redeploy**.

5. Click **Next**.

The Select Archive page is displayed.

6. In the Archive or Exploded Directory section, you can select one of the following:

- **Use the archive or exploded directory in the existing source location of the application on the Administration Server.**
- **Archive is on the machine where this browser is running.** Enter the location of the archive or click **Browse** to find the archive file.

- **Archive or exploded directory is on the server where Enterprise Manager is running.** Enter the location of the archive or click **Browse** to find the archive file.
- 7. In the Deployment Plan section, you can select one of the following:
 - **Create a new deployment plan when deployment configuration is done.**
 - **Deployment plan is on the machine where this web browser is running.** Enter the path to the plan.
 - **Deployment plan is on the server where Enterprise Manager is running.** Enter the path to the plan.
- 8. Click **Next**.
The Application Attributes page is displayed.
- 9. In the Application Attributes section, for **Application Name**, enter the application name.
- 10. In the Context Root of Web Modules section, if the Web module does not have the context root configured in the application.xml file, you can specify the context root for your application. The context root is the URI for the Web module. Each Web module or EJB module that contains Web services may have a context root.
- 11. The Target Metadata Repository section is displayed. In this section, you can choose the repository and partition for this application:
 - To change the repository, click the icon next to the **Repository Name**. In the Metadata Repositories dialog box, select the repository and click **OK**.
 - To change the partition, enter the partition name in **Partition Name**. Oracle recommends that you create a new partition for each application. If you enter a name of a partition that does not exist, the partition is created.
- 12. If the application's adf-config.xml file archive contains MDS configuration for an MDS shared repository, the Shared Metadata Repository section is displayed. In this section, you can choose the repository and partition for this application.
- 13. Click **Next**.
The Deployment Settings page is displayed.
- 14. On this page, you can perform common tasks before deploying your application or you can edit the deployment plan or save it to a disk. In the Deployment Tasks section, you can:
 - Configure Web modules
 - Configure application security
 - Configure persistence

See [Section 10.7](#) for detailed information about these options.
- 15. Expand **Deployment Plan**.
You can edit and save the deployment plan, if you choose.
- 16. Click **Deploy**.
Fusion Middleware Control displays processing messages.
- 17. When the deployment is completed, click **Close**.
- 18. In the Confirmation page, click **Redeploy**.

10.5 Deploying, Undeploying, and Redeploying SOA Composite Applications

SOA composite applications consist of the following:

- Service components such as Oracle Mediator for routing, BPEL processes for orchestration, human tasks for workflow approvals, business rules for designing business decisions, and complex event processing for queries of event streams
- Binding components (services and references) for connecting SOA composite applications to external services, applications, and technologies

These components are assembled together into a SOA composite application. This application is a single unit of deployment that greatly simplifies the management and lifecycle of SOA applications.

You can use Fusion Middleware Control, Oracle JDeveloper, or the command line to deploy, undeploy, or redeploy a SOA application. The following topics describe using Fusion Middleware Control to accomplish these tasks:

- [Deploying SOA Composite Applications](#)
- [Undeploying SOA Composite Applications](#)
- [Redeploying SOA Composite Applications](#)

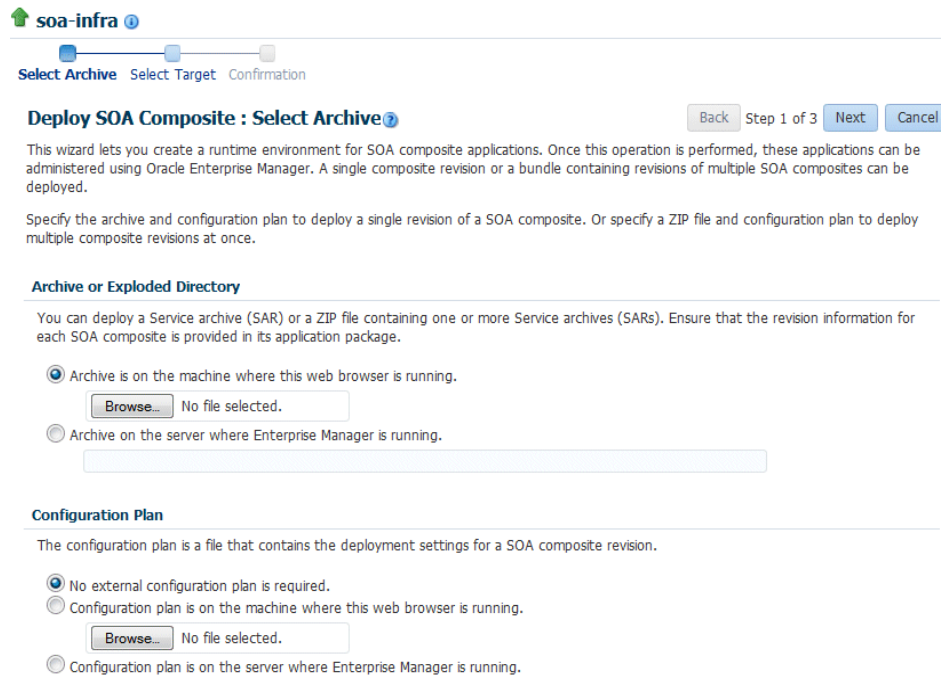
See Also: *Administering Oracle SOA Suite and Oracle Business Process Management Suite*

10.5.1 Deploying SOA Composite Applications

When you deploy a SOA composite application, the deployment extracts and activates the composite application in the SOA Infrastructure.

You can deploy SOA composite applications from Fusion Middleware Control with the Deploy SOA Composite wizard:

1. From the navigation pane, expand **SOA**, and then select **soa-infra**.
The SOA Infrastructure home page is displayed.
2. From the SOA Infrastructure menu, choose **SOA Deployment**, then **Deploy**.
The Deployment Wizard, Select Archive page is displayed, as shown in the following figure:



3. In the Archive or Exploded Directory section, you can select one of the following:
 - **Archive is on the machine where this browser is running.** Enter the location of the archive or click **Browse** to find the archive file.
 - **Archive or exploded directory is on the server where Enterprise Manager is running.** Enter the location of the archive or click **Browse** to find the archive file.
 You can specify the archive of the SOA composite application to deploy. The archive contains the project files of the application to be deployed (for example, **HelloWorld_rev1.0.jar** for a single archive or **OrderBooking_rev1.0.zip** for multiple archives).
4. In the Configuration Plan section, optionally specify the configuration plan to include with the archive. The configuration plan enables you to define the URL and property values to use in different environments. During process deployment, the configuration plan is used to search the SOA project for values that must be replaced to adapt the project to the next target environment.
5. Click **Next**.
 The Select Target page appears.
6. In the SOA Partition section, select the partition into which to deploy this SOA composite application. Partitions enable you to logically group SOA composite applications into separate sections. Note that even if there is only one partition available, you must explicitly select it. Once deployed, a composite cannot be transferred to a different partition.
7. Click **Next**.
 The Confirmation page appears.
8. Review your selections.
9. Select whether or not to deploy the SOA composite application as the default revision. The default revision is instantiated when a new request comes in.

10. Click Deploy.

Processing messages are displayed.

11. When deployment has completed, close the confirmation box.

See Also: "Deploying Applications" in *Administering Oracle SOA Suite and Oracle Business Process Management Suite* for complete information about deploying SOA Composite applications

10.5.2 Undeploying SOA Composite Applications

You can undeploy SOA composite applications from Fusion Middleware Control with the Undeploy SOA Composite wizard:

1. From the navigation pane, expand **SOA**, and then select **soa-infra**.
The SOA Infrastructure home page is displayed.
2. From the SOA Infrastructure menu, choose **SOA Deployment**, then **Undeploy**.
3. Select the composite to undeploy and click **Next**.
4. Review your selections. If you are satisfied, click **Undeploy**.
Processing messages are displayed.
5. When undeployment has completed, close the confirmation window.

See Also: "Undeploying Applications" in *Administering Oracle SOA Suite and Oracle Business Process Management Suite* for complete information about undeploying SOA Composite applications

10.5.3 Redeploying SOA Composite Applications

You can redeploy SOA composite applications from Fusion Middleware Control with the Redeploy SOA Composite wizard:

1. From the navigation pane, expand **SOA**, and then select **soa-infra**.
The SOA Infrastructure home page is displayed.
2. From the SOA Infrastructure menu, choose **SOA Deployment**, then **Redeploy**.
The Select Composite page is displayed.
3. Select the composite that you want to redeploy.
4. Click **Next**.
The Select Archive page appears.
5. In the Archive or Exploded Directory section, select the location of the SOA composite application revision you want to redeploy.
6. In the Configuration Plan section, optionally specify the configuration plan to include with the archive.
7. Click **Next**.
The Confirmation page appears.
8. Select whether or not to redeploy the SOA composite application as the default revision.
9. Click **Redeploy**.

Processing messages are displayed.

10. When redeployment has completed, click **Close**.

See Also: "Redeploying Applications" in *Administering Oracle SOA Suite and Oracle Business Process Management Suite* for complete information about redeploying SOA Composite applications

10.6 Managing Deployment Plans

A **deployment plan** is a client-side aggregation of all the configuration data needed to deploy an archive into Oracle WebLogic Server. A deployment plan allows you to easily deploy or redeploy an application using a saved set of configuration settings.

A new deployment plan is created by default if you do not apply an existing deployment plan to an application at the time of deployment, as described in [Section 10.3.1](#). Once created, you can save a deployment plan as a file and reuse it for redeploying the application or for deploying other applications.

However, if you change the configuration of an application after it is deployed (for example, if you modify the MDS configuration of an application), then any existing deployment plans you saved no longer represent the configuration settings of the deployed application.

In such a situation, you can fetch a new deployment plan that more closely represents the configuration of the deployed application.

To fetch the deployment plan of an application that is currently deployed:

1. From the **WebLogic Domain** menu, choose **Deployments**.
2. Select an application from the list of currently deployed applications.
3. Click **Fetch Deployment Plan**.

The Fetch Deployment Plan page is displayed.

4. Select a location where you want to save the deployment plan, and click **Fetch**.

You can save the plan to the computer where the Web browser is running or to the computer where Fusion Middleware Control is running.

5. In the resulting dialog box, specify a directory location for the saved deployment plan.

You can now use this deployment plan to later deploy or redeploy the application using the configuration currently in use by the application.

Alternatively, you can edit a deployment plan on the Deployment Settings page of the Application Deployment wizard.

10.7 About the Common Deployment Tasks in Fusion Middleware Control

When you deploy an application using Fusion Middleware Control, you can use the Deployment Settings page of the Deployment wizard to perform specific deployment configuration tasks before the application is deployed.

The following describes the deployment tasks that can appear on the Deployment Settings page, depending on the type of application you are deploying.

Configure Web modules

This deployment task is available when you are deploying any application that includes a Web module. In most cases, this means the application contains a Web application deployment descriptor (web.xml or weblogic.xml); however, a Web module can also be identified by annotations in the Java code of the application.

You can use this deployment task to set standard Web application deployment descriptor properties, such as:

- Session validation interval
- Maximum age of session cookies

Configure EJBs

This deployment task is available for any application that includes an EJB module. In most cases, this means the application contains an EJB deployment descriptor (ejb-jar.xml or weblogic-ebj-jar.xml); however, an EJB module can also be identified by annotations in the Java code of the application.

You can use this deployment task to set standard EJB deployment descriptor properties, such as:

- The maximum number of beans in the free pool
- The EJB network access point

Configure Application Security

This deployment task is available for all application types. However, the options available when you select this task vary depending on the existence of the following files in the application:

- jazn-data.xml

If the jazn-data.xml file exists in the application, then you can:

- Append, overwrite, or ignore policy migration.
 - * If you are deploying the application for the first time, then select **Append**.
 - * If the application was previously deployed and the application authorization policy exists, then select **Append**, or select **Ignore** to keep the application authorization policy.
 - * To overwrite the previous policy, then select **Overwrite**.
- Specify the Application stripe ID, if the stripe ID is inconsistent with the one defined in the migration options.
- Specify that policies are removed when the application is undeployed.

- cwallet.sso

If an cwallet.sso file exists in the application, then you can set additional application credential migration options.

If the application contains both files, the page displays both sections.

For more information about the settings available when you select the Configure Application Security deployment task, see "Deploying Java EE and Oracle ADF Applications with Fusion Middleware Control" in *Securing Applications with Oracle Platform Security Services*.

If neither of these files exists in the application, then you can use this task to determine how user roles and policies will be defined when the application is deployed. For

example, you can choose to use only the roles and policies defined in the deployment descriptors, or you can choose to use only the roles and policies defined on the server. The Configure Application Security page displays the following options:

- **Deployment Descriptors Only:** Use only roles and policies that are defined in the deployment descriptors.
- **Custom Roles:** Use roles that are defined in the Administration Console; use policies that are defined in the deployment descriptor.
- **Custom Roles and Policies:** Use only roles and policies that are defined in the Administration Console.
- **Advanced:** Use a custom model that you have configured on the realm's configuration page.

Configure persistence

This deployment task is available for applications that contain one or more persistence.xml files. Using this task, you can configure the Java Persistent API (JPA) persistence units for the application.

You can view details about each persistence unit and define a Java Transaction API (JTA) data source or non-JTA data source for each persistence unit.

Configuring the data sources for persistence units can be useful for applications that take advantage of Oracle TopLink. For more information, refer to the *Solutions Guide for Oracle TopLink*.

For more information about how persistence units and the persistence.xml file can be used in Java EE applications, refer to the definition of Persistence Units in the Java EE 5 Tutorial at the following Web site:

<http://download.oracle.com/javaee/5/tutorial/doc/bnbqw.html#bnbrj>

Configure ADF connections

This deployment task is available for applications that use ADF connections. You can modify the connection information for an external application. For more information about ADF connections, see *Developing Fusion Web Applications with Oracle Application Development Framework*.

10.8 Changing MDS Configuration Attributes for Deployed Applications

If your application uses an MDS Repository, you can modify configuration attributes after the application is deployed. To view or modify the attributes, you can use the System MBean Browser or WLST.

Note: Changes to the configuration persist in MDS as customizations. Because these persist as customizations:

- Any changes made to the configuration are retained across application deployments. For example, assume that an application has an `ExternalChangeDetectionInterval` configuration attribute value set to 40 seconds through Oracle JDeveloper. If you change the `ExternalChangeDetectionInterval` configuration attribute to 50 seconds, and you redeploy the application, the value of the attribute remains at 50 seconds.
 - In a cluster, because all instances of the deployed application point to the same MDS Repository partition, all instances of the application use the same value. If a configuration attribute has been changed for one application instance, all instances of that application in a cluster use the changed value.
-
-

The following topics describe how you can change the MDS configuration attributes:

- [Changing the MDS Configuration Attributes Using Fusion Middleware Control](#)
- [Changing the MDS Configuration Using WLST](#)
- [Restoring the Original MDS Configuration for an Application](#)

10.8.1 Changing the MDS Configuration Attributes Using Fusion Middleware Control

To change the MDS configuration attributes of an application, take the following steps:

1. Navigate to the application's home page by expanding **Application Deployments**. Then, select an application.

The application's home page is displayed.

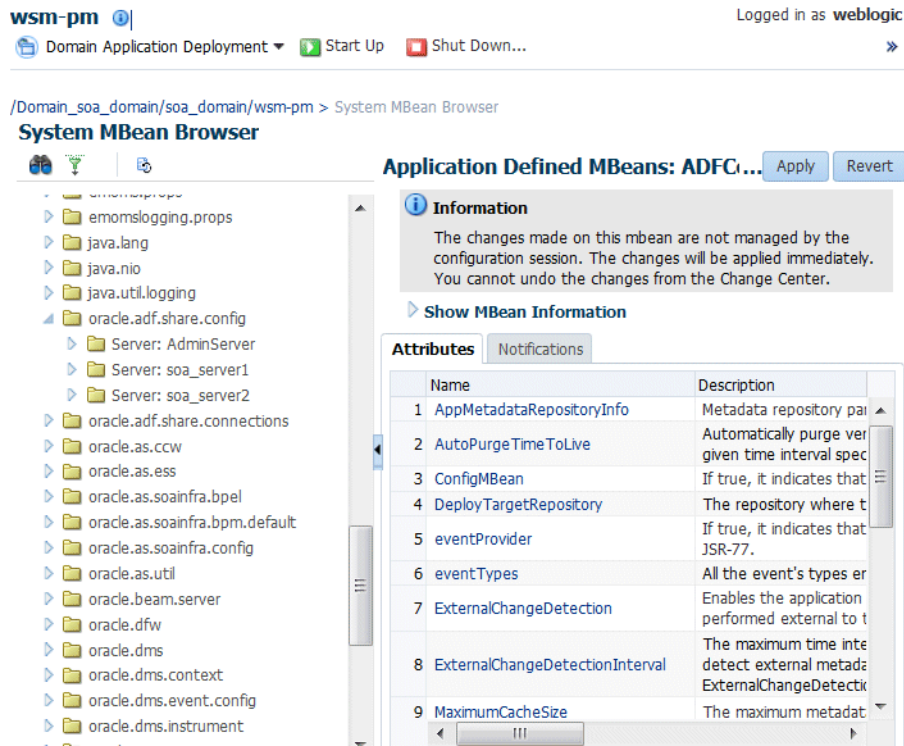
2. From the Application Deployment menu, choose **System MBean Browser**.

The System MBean Browser page is displayed.

3. Expand **Application Defined MBeans**, then **oracle.adf.share.config**, then **Server: name**, then **Application: name**, then **ADFConfig**, then **ADFConfig**, and **ADFConfig**.

4. Select **MDSAppConfig**.

The Application Defined MBeans page is displayed, as shown in the following figure:



5. You can view the description and values for the attributes.

Table 10–2 describes the configuration attributes that are specific to MDS. Note that other attributes, such as ConfigMBean appear in the browser, but these are generic attributes for all MBeans.

Table 10–2 MDS Configuration Attributes for Deployed Applications

Attribute	Description
AppMetadataRepositoryInfo	Read only. Describes the metadata repository partition where the application is deployed.
AutoPurgeTimeToLive	Automatically purge versions of metadata documents older than the given time interval, specified in seconds. Any unlabeled versions older than this time interval are automatically purged on any subsequent update from this application. If the value is not set, versions are not automatically purged.
ConfigMBean	If true, indicates that this MBean is a Config MBean.
DeployTargetRepository	The name of the target repository configured for the application.
eventProvider	If true, it indicates that this MBean is an event provider as defined by JSR-77.
eventTypes	All the event's types emitted by this MBean.

Table 10–2 (Cont.) MDS Configuration Attributes for Deployed Applications

Attribute	Description
ExternalChangeDetection	<p>Specifies that the MDS Repository is polled to determine if any metadata changes have been performed on other cluster nodes or by other applications. If changes are detected, notifications are sent to applications that share the repository.</p> <p>Multiple applications can share metadata that is deployed to a shared repository. Changes performed by one application to this shared metadata can be detected by the other application. To do this, all of the applications should configure the shared repository as part of their application configuration.</p> <p>If the MDS Repository is being used by more than one application in the same JVM, then MDS polls for changes if any of those applications have ExternalChangeDetection set to true.</p> <p>This attribute should only be set to false if the application metadata is never updated or if it is used only by this application and on a single server node.</p> <p>This attribute is applicable only to database-based repositories. The default is true.</p>
ExternalChangeDetectionInterval	<p>The maximum time interval, in seconds, to poll the MDS Repository to determine if there are external metadata changes. This attribute is only valid if ExternalChangeDetection is enabled.</p> <p>If the MDS Repository is shared and being used by more than one application in the same JVM, MDS uses the lowest of the values specified in the different applications for this attribute. As a result, changing the value of this parameter in one application only has an effect if the new value is lower than any values specified in the other applications.</p> <p>The default is 30 seconds.</p>
MaximumCacheSize	<p>The maximum metadata cache size limit, in kilobytes. If the value is 0, caching is disabled. If no value is specified, there is no cache limit. In this case, cached data is stored indefinitely.</p>
objectName	<p>All the event's types emitted by this MBean.</p>
ReadOnly	<p>If true, it indicates that this MBean is a read-only MBean.</p>
ReadOnlyMode	<p>Changes the application to read-only mode, so that no updates can be made to the application's repository partition, including configuration and application metadata.</p>
RemoteNotifications	<p>Enables distributed remote notifications of applicable metadata changes. This parameter is valid only if ExternalChangeDetection is enabled.</p>
RestartNeeded	<p>Enables distributed remote notifications of applicable metadata changes. This parameter is only valid if ExternalChangeDetection is enabled.</p>
RetryConnection	<p>Enables the application to retry the connection to the metadata repository after connection failure.</p>
SharedMetadataRepositoryInfo	<p>Read only. Specifies the MDS Repository partition used by the application. Note that an application can use more than one shared metadata repository.</p>
stateManageable	<p>If true, it indicates that this MBean provides State Management capabilities as defined by JSR-77.</p>

Table 10–2 (Cont.) MDS Configuration Attributes for Deployed Applications

Attribute	Description
statisticsProvider	If true, it indicates that this MBean is a statistic provider as defined by JSR-77.
SystemMBean	If true, it indicates that this MBean is a System MBean.
Visible	If true, it indicates that this MBean is visible to the current user.

6. To view or modify an attribute, select the attribute.
The attribute page is displayed.
7. If the attribute is not read-only, you can change the values. For example, for AutoPurgeTimeToLive, you can change the interval, by entering a new value in **Value**.
8. Click **Apply**.
9. Navigate up to ADFConfig (the parent of MDSAppConfig) and select it.
10. In the Operations tab, click **Save**.
11. Click **Invoke**.

10.8.2 Changing the MDS Configuration Using WLST

You can change the MDS configuration of an application using WLST. The following example shows a WLST script that reads and then sets the ReadOnlyMode attribute:

```

"""
Getting ReadOnlyMode Attribute from MBean
"""
connect('username', 'password', 'hostname:port')
application = 'application_name'
attribute = 'ReadOnlyMode'
beanName = 'oracle.adf.share.config:ApplicationName='+ application
+',name=MDSAppConfig,type=ADFConfig,Application='+ application
+',ADFConfig=ADFConfig,*'

beanObjectName = ObjectName(beanName)
beans = mbs.queryMBeans(beanObjectName, None)
bean = beans.iterator().next().getObjectInstance()
custom()
value = mbs.getAttribute(bean, attribute)
print value

"""
Setting ReadOnlyMode Attribute from MBean
"""
attr = Attribute(attribute, Boolean(0))
mbs.setAttribute(bean, attr)
value = mbs.getAttribute(bean, attribute)
print value

"""
Saving the Changes. This is required to persist the changes.
"""

adfConfigName = 'oracle.adf.share.config:ApplicationName='+ application +

```

```
',name=ADFConfig,type=ADFConfig,Application='+ application + ',*'
adfConfigObjectName = ObjectName(adfConfigName)
adfConfigMBeans = mbs.queryMBeans(adfConfigObjectName, None)
adfConfigMBean = adfConfigMBeans.iterator().next().getObjectInstance()
mbs.invoke(adfConfigMBean, 'save', None, None)
```

10.8.3 Restoring the Original MDS Configuration for an Application

To restore the original MDS configuration for an application:

1. Navigate to the application's home page by expanding **Application Deployments**. Then, select an application.

The application's home page is displayed.

2. From the Application Deployment menu, choose **System MBean Browser**.

The System MBean Browser page is displayed.

3. Expand **Application Defined MBeans**, then **oracle.adf.share.config**, then **Server: name**, then **Application: name**, then **ADFConfig**, and then **ADFConfig**.

4. Select the Operations tab.

5. Select **RestoreToOriginalConfiguration**.

The Operation: restoreToOriginalConfiguration page is displayed.

6. Click **Invoke**.

Use this operation with caution. It causes all changes made to the original `adf-config.xml` file to be discarded. The `adf-config.xml` is restored to the base document.

Part V

Monitoring Oracle Fusion Middleware

This part provides information about how to find information about the cause of an error and its corrective action, to view and manage log files to assist in monitoring system activity and to diagnose problems and how to monitor Oracle Fusion Middleware.

Part V contains the following chapters:

- [Chapter 11, "Monitoring Oracle Fusion Middleware"](#)
- [Chapter 12, "Managing Log Files and Diagnostic Data"](#)
- [Chapter 13, "Diagnosing Problems"](#)

Monitoring Oracle Fusion Middleware

This chapter describes how to monitor Oracle Fusion Middleware using Fusion Middleware Control, Oracle WebLogic Server Administration Console, and the command line.

It describes the following sections:

- [Section 11.1, "Monitoring the Status of Oracle Fusion Middleware"](#)
- [Section 11.2, "Viewing the Performance of Oracle Fusion Middleware"](#)
- [Section 11.3, "Viewing the Routing Topology"](#)

11.1 Monitoring the Status of Oracle Fusion Middleware

Monitoring the health of your Oracle Fusion Middleware environment and ensuring that it performs optimally is an important task for the administrator.

Oracle Fusion Middleware provides the following methods for monitoring the status of your environment:

Oracle Fusion Middleware provides the following methods for monitoring the status of your environment:

- **Fusion Middleware Control:** You can monitor the status of Oracle WebLogic Server domains, clusters, servers, Java components, system components, and applications. Navigate to the entity's home page, for example, to the home page for an Oracle HTTP Server instance.
- **Oracle WebLogic Server Administration Console:** You can monitor the status of Oracle WebLogic Server domains, clusters, servers, Java components, and applications. From the Administration Console, navigate to the entity's page. See "Overview of the Administration Console" in *Understanding Oracle WebLogic Server* for information on monitoring using the console.
- **The command line:** You can monitor the status of your environment using the WLST state command.

Most of the monitoring tasks in this chapter describe how to monitor using Fusion Middleware Control or the command line.

The following topics provide more detail:

- [Monitoring an Oracle WebLogic Server Domain](#)
- [Monitoring an Oracle WebLogic Server Administration or Managed Server](#)
- [Monitoring a Cluster](#)
- [Monitoring a Java Component](#)

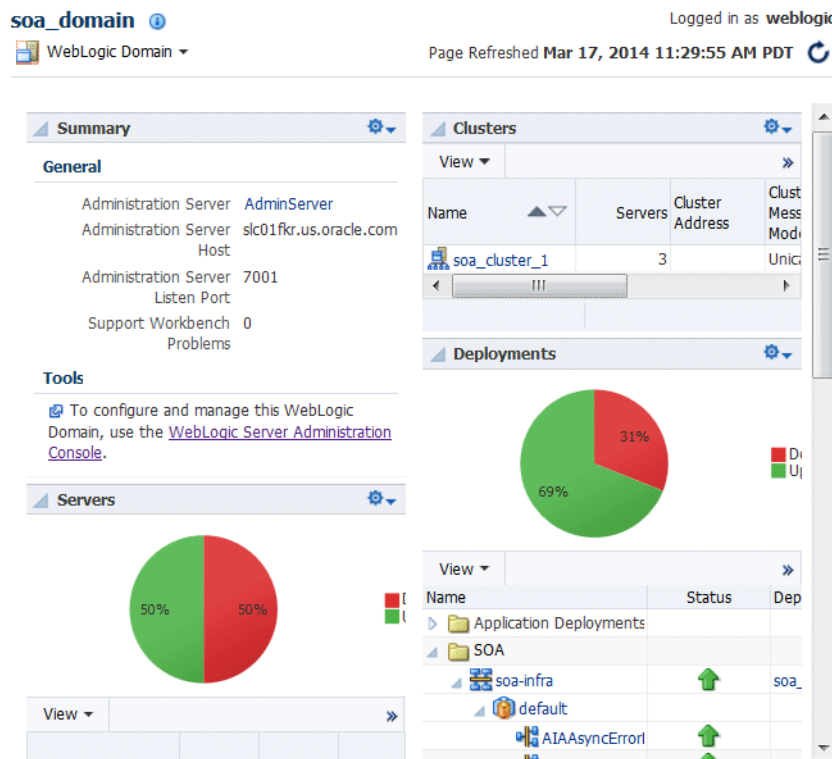
- [Monitoring a System Component](#)
- [Monitoring Java EE Applications](#)
- [Monitoring ADF Applications](#)
- [Monitoring SOA Composite Applications](#)
- [Monitoring Applications Deployed to a Cluster](#)
- [Monitoring the Status of Components Using the Command Line](#)

11.1.1 Monitoring an Oracle WebLogic Server Domain

You can view the status of a domain, including the servers, clusters, and deployments in the domain from the domain home page of Fusion Middleware Control:

1. From the WebLogic Domain menu, select **Home**.

The domain home page is displayed, as shown in the following figure:



This page shows the following:

- A general summary of the domain, along with a link to the Oracle WebLogic Server Administration Console
- Information about the servers, both the Administration Server and the Managed Servers, in the domain
- Information about the clusters in the domain
- Information about the deployments in the domain
- A Resource Center, which provides links to more information

For information about monitoring an Oracle WebLogic Server domain using the Oracle WebLogic Server Administration Console, see "Overview of the Administration

Console" in *Understanding Oracle WebLogic Server*. The Administration Console provides details about the health and performance of the domain.

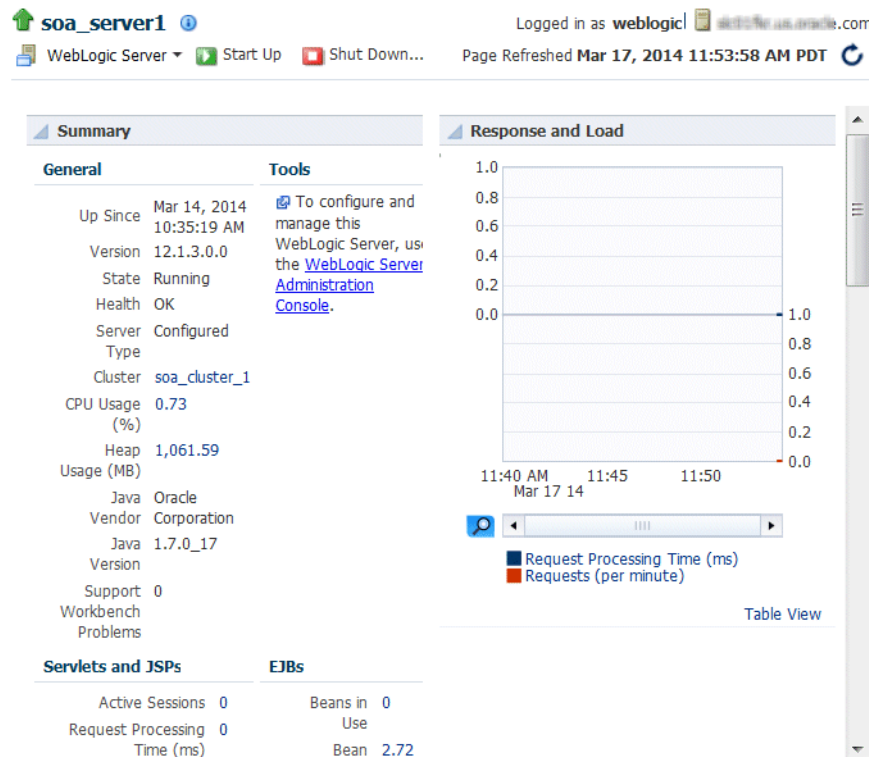
11.1.2 Monitoring an Oracle WebLogic Server Administration or Managed Server

You can view the status of a WebLogic Server Administration Server or Managed Server in Fusion Middleware Control:

1. From the navigation pane, expand the domain.
2. Select the server.

The server home page is displayed.

The following figure shows the home page for a Managed Server:



This page shows the following:

- A general summary of the server, including its state, and information about the servlets, JSPs, and EJBs running in the server
- Response and load
- Information about the applications deployed to the server

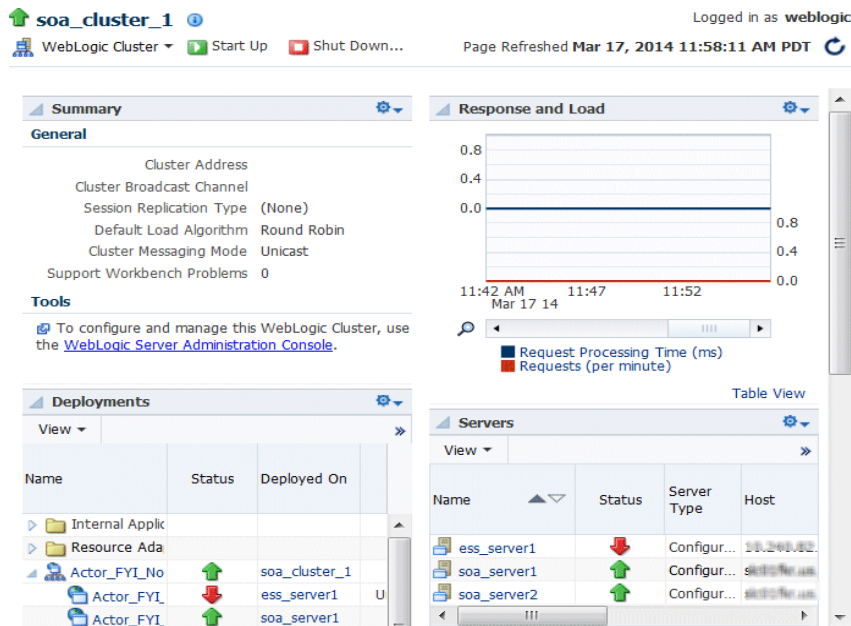
For information about monitoring servers using the Oracle WebLogic Server Administration Console, see "Overview of the Administration Console" in *Understanding Oracle WebLogic Server*. The Administration Console provides details about the health and performance of the server.

11.1.3 Monitoring a Cluster

You can view the status of a cluster, including the servers and deployments in the cluster using Fusion Middleware Control:

1. From the navigation pane, expand the domain.
2. Select the cluster.

The cluster page is displayed, as shown in the following figure:



This page shows the following:

- A general summary of the cluster, including the broadcast channel, if appropriate, the load algorithm, and the messaging mode
- A response and load section, which shows the requests per minute and the request processing time
- A deployments section with information about the applications deployed to the cluster
- A servers section, with a table listing the servers that are part of the cluster

See Also: "Overview of the Administration Console" in *Understanding Oracle WebLogic Server* for information about monitoring a cluster using Oracle WebLogic Server Administration Console. The Administration Console provides details about the health and performance of the cluster.

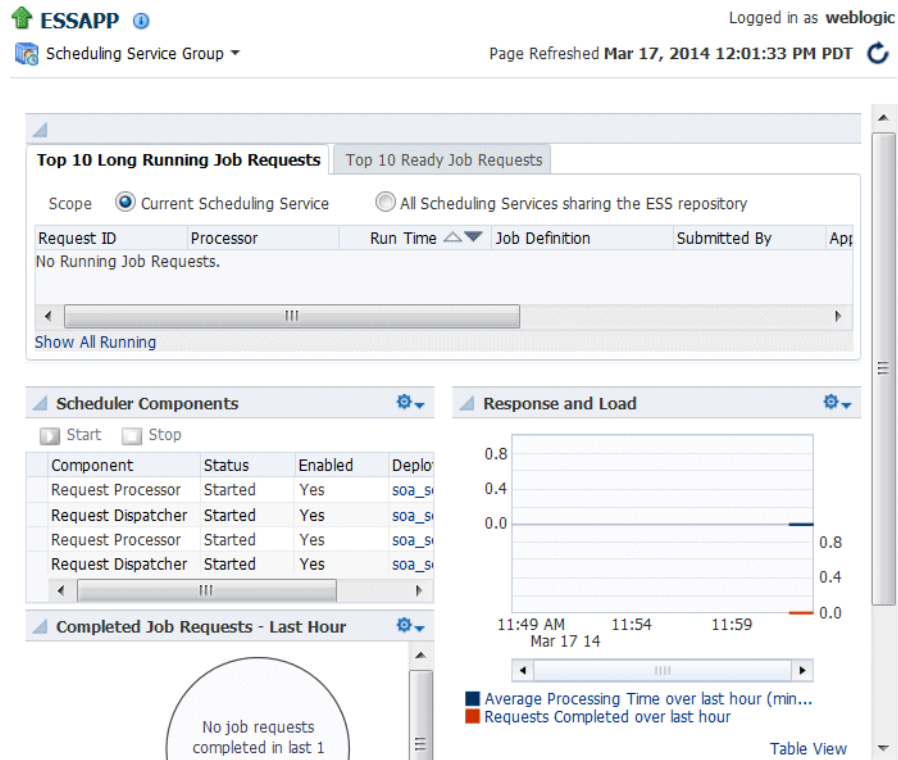
11.1.4 Monitoring a Java Component

You can view the status of a Java component, including whether the component is started, in the component home page in Fusion Middleware Control.

To monitor a Java component, such as Oracle Enterprise Scheduler:

1. From the navigation pane, expand the type of component, such as Scheduling Services.
2. Select the component. For example, select the ESSAPPinstance.

The component home page is displayed, as shown in the following figure:



This page shows the following:

- The top 10 long running job requests
- Scheduler components
- A chart showing response and load
- Completed Job Requests in the last hour.

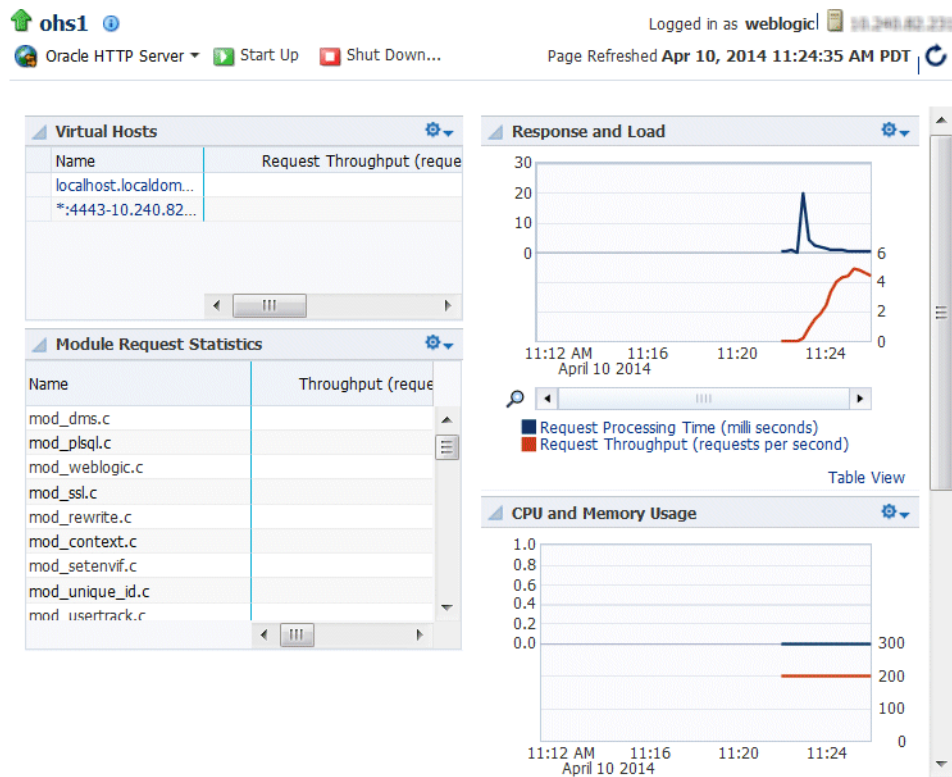
See Also: "Overview of the Administration Console" in *Understanding Oracle WebLogic Server* for information about using the Oracle WebLogic Server Administration Console to monitor Java components

11.1.5 Monitoring a System Component

To monitor a system component, such as Oracle HTTP Server:

1. From the navigation pane, expand the component type, such as **HTTP_Server**.
2. Select the component, such as ohs1.

The component home page is displayed, as shown in the following figure:



This page shows the following:

- A response and load section, which shows the requests per second and the request processing time
- CPU and memory usage
- The virtual hosts, with their names, request throughput and response size.
- Module request statistics, with a list of modules and the throughput for each.: A table listing the processing time for each module
- A Resource Center with links to relevant documentation

11.1.6 Monitoring Java EE Applications

To monitor a Java EE application using Fusion Middleware Control:

1. From the navigation pane, expand **Application Deployments**, then select the application to monitor.

The application's home page is displayed.

2. In this page, you can view a summary of the application's status, entry points to the application, Web services and modules associated with the application, and the response and load.

The following figure shows a portion of the application's home page:

testapp1a ⓘ Logged in as weblogic

Domain Application Deployment ▼ Start Up Shut Down... Page Refreshed Mar 17, 2014 12:51:26 PM PDT ↻

Summary ⓘ ⚙️

General

State Active
Health OK
Source Path /scratch/oracle1/Oracle/domains/soa_domain/sysman/upload/deploy/testapp1a/archive/testapp1a.ear
Staging Mode (not specified)
Plan (not specified)
Staging Mode
Security Model DDOnly
Application Type Enterprise Application

Modules ⓘ ⚙️

Name	Module Type
testapp1-web.war	Web Application

Web Services ⓘ ⚙️

Name	Server	Application
No Web Services Found		

Deployments ⓘ ⚙️

View ▼

Name	Status
testapp1a	↑

Data Sources ⓘ ⚙️

This page shows the following:

- A summary of the application, including its state, and information about active sessions, active requests, and request processing time
- A Deployments section, with the application and its status.
- A list of modules with the type of module for each

11.1.7 Monitoring ADF Applications

To monitor an ADF application:

1. From the navigation pane, expand **Application Deployments**, then select the application to monitor.

The application's home page is displayed.

The following figure shows a portion of the application's home page:

mdsappdb1 ⓘ Logged in as weblogic

Domain Application Deployment ▼ ▶ Start Up ▶ Shut Down... Page Refreshed Mar 17, 2014 12:57:11 PM PDT ↻

General

State Active

Health OK

Source Path /scratch/oracle1/Oracle/domains/soa_domain/sysman/upload/deploy/mdsappdb1/archive/mdsappdb1.ear

Staging Mode (not specified)

Plan (not specified)

Staging Mode

Security Model DDOnly

Application Type Enterprise Application

mdsappdbweb.war Web Application

Web Services ⚙️

Name	Server	Application
No Web Services Found		

Deployments ⚙️

View ▼

Name	Status
mdsappdb1	▶

Data Sources ⚙️

Name	Location
No datasources found	

- A summary of the application, including its state, the Managed Server on which it is deployed, and information about active sessions, active requests, and request processing time
 - Deployments, which lists the servers on which the application is deployed.
 - A list of modules with the type of module for each
 - A list of data sources
2. To view health of the environment, from the **Application Deployments** menu choose **Monitoring**, then **Environment Monitoring**. The Environment Monitoring page is displayed.

It contains tabs for Health, Query Caching, Workload, and Coherence.

11.1.8 Monitoring SOA Composite Applications

To monitor a SOA composite application:

1. From the navigation pane, expand **SOA**, then **soa-infra**. Select the application to monitor.

The application's home page is displayed.

2. From this page, you can monitor the running instances, faults and rejected messages, and component metrics.

The following figure shows part of a SOA composite home page:

CustomerService [1.0] | SOA Composite | Logged in as weblogic | Page Refreshed Mar 19, 2014 7:44:04 AM PDT

Active | Retire... | Shut Down... | Test | Settings... | Related Links

Dashboard | Composite Definition | Flow Instances | Unit Tests | Policies

Components

Name	Component Type
GetCustomersBPEL	BPEL
DeleteCustomerBPEL	BPEL
GetCustomerBPEL	BPEL
PutCustomerBPEL	BPEL
CustomerMediatorService	Mediator

Services and References

Name	Type	Usage	Total Messages	Average Processing Time (sec)
CustomerMediatorService_ep	Web Service	Service	0	0.000
CustomerRestService	REST Binding	Service	0	0.000
CustomerServiceAdapter	JCA Adapter	Reference	0	0.000

This page, with the Dashboard tab selected, shows the following:

- A table containing a list of composites
- A table containing services and references

11.1.9 Monitoring Applications Deployed to a Cluster

If you deploy an application to a cluster, Oracle Fusion Middleware automatically deploys the application to each Managed Server in the cluster. As a result, there is an instance of the application on each server.

There are times when you want to monitor the performance of the application on an individual server, and times when you want to monitor the overall performance of the application across all the servers in the cluster.

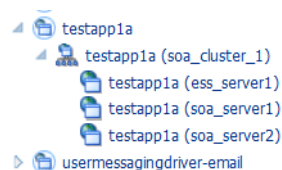
For example, normally, you would manage the overall performance of the application to determine if there are any performance issues affecting all users of the application, regardless of which instance users access. If you notice a performance problem, you can then drill down to a specific instance of the application to determine if the problem is affecting one or all of the application instances in the cluster.

Fusion Middleware Control provides monitoring pages for both of these scenarios:

1. From the navigation pane, expand **Application Deployments**.

Fusion Middleware Control lists the applications deployed in the current domain.

2. If an application has been deployed to a cluster, expand the application in the navigation pane. Fusion Middleware Control shows that it is deployed to the cluster to indicate that it represents more than one instance of the application on the cluster:



3. Monitor the overall performance of the application on the cluster by clicking the cluster application, or monitor the performance of the application on a single server by clicking one of the application deployment instances.

11.1.10 Monitoring the Status of Components Using the Command Line

To monitor the status of components using the WLST command line:

- For Java components, use the WLST `state` command, with the following format:

```
state(name, type)
```

For example, to get the status of the Managed Server `server1`, use the following command:

```
wls:/mydomain/serverConfig> state('server1','Server')
Current state of "server1": SUSPENDED
```

- To monitor the status of system components, use the WLST `state` command, with the following format:

Oracle Fusion Middleware provides the following methods for monitoring the status of your environment:

To monitor the status of system components, use the WLST `state` command, with the following format:

```
state('component_name']]
```

For example, to view the status `ohs1`, use the following command:

```
state('ohs1']]
```

11.2 Viewing the Performance of Oracle Fusion Middleware

If you encounter a problem, such as an application that is running slowly or is hanging, you can view more detailed performance information, including performance metrics for a particular target, to find out more information about the problem.

Oracle Fusion Middleware automatically and continuously measures run-time performance. The performance metrics are automatically enabled; you do not need to set options or perform any extra configuration to collect them.

Note that Fusion Middleware Control provides real-time data. If you are interested in viewing historical data, consider using Oracle Enterprise Manager Grid Control.

For example, to view the performance of an Oracle WebLogic Server Managed Server:

1. From the navigation pane, expand the domain.
2. Select the server to monitor.

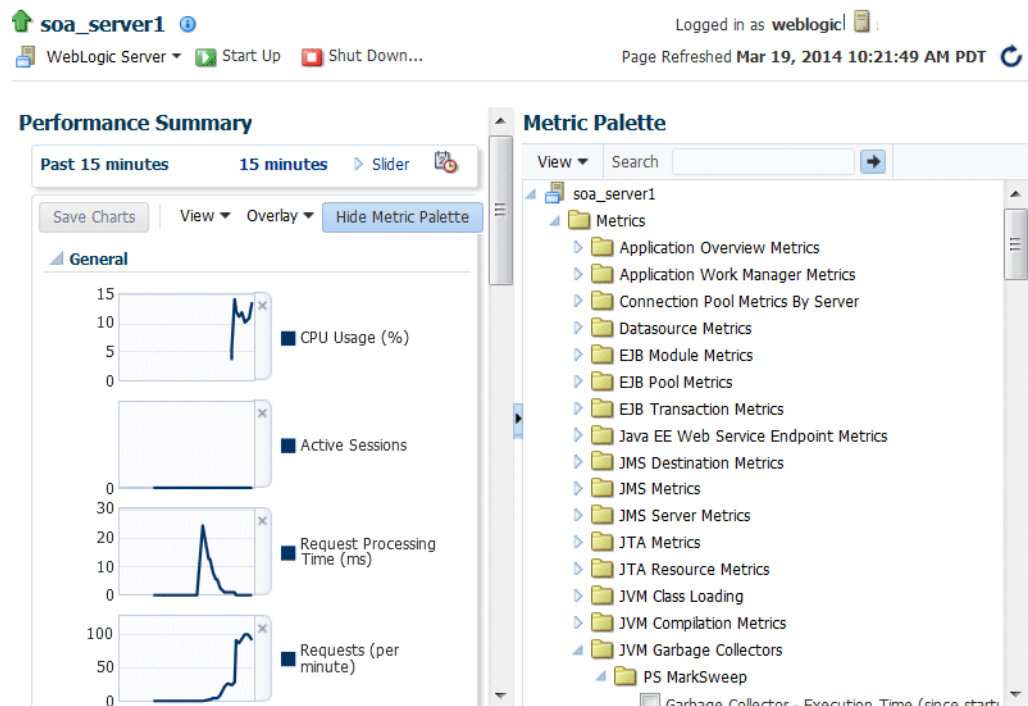
The Managed Server home page is displayed.

3. From the WebLogic Server menu, choose **Monitoring**, then **Performance Summary**.

The Performance Summary page is displayed. It shows performance metrics, as well as information about response time and request processing time for applications deployed to the Oracle WebLogic Server.

4. To see additional metrics, click **Show Metric Palette** and expand the metric categories.

The following figure shows the Performance Summary page with the Metric Palette displayed:



5. Select a metric to add it to the Performance Summary.
6. To overlay another target, click **Overlay**, and select the target. The target is added to the charts, so that you can view the performance of more than one target at a time, comparing their performance.
7. To customize the time frame shown by the charts, you can:
 - Click **Slider** to display a slider tool that lets you specify that more or less time is shown in the charts. For example, to show the past 10 minutes, instead of the past 15 minutes, slide the left slider control to the right until it displays the last 10 minutes.
 - Select the calendar and clock icon. Then, enter the **Start Time** and **End Time**. If there is no data available for those times, a confirmation message displays, explaining the timeline will be automatically adjusted to the time period for which the data is available.

You can also view the performance of a components, such as Oracle HTTP Server or Oracle SOA Suite. Navigate to the component and select **Monitoring**, then **Performance Summary** from the dynamic target menu.

11.3 Viewing the Routing Topology

Fusion Middleware Control provides a Topology Viewer for the domain. The Topology Viewer is a graphical representation of routing relationships across components and elements of the domain. You can easily determine how requests are routed across components. For example, you can see how requests are routed from Oracle HTTP Server, to a Managed Server, to a data source.

Note: To view relationships between Oracle WebLogic Server and Oracle HTTP Server, each target must be running and show its status as Up.

The Topology Viewer enables you to easily monitor your Oracle Fusion Middleware environment. You can see which entities are up and which are down.

You can also print the topology.

To view the topology:

1. From the WebLogic Domain menu, click **Routing Topology**.

The Routing Topology page is displayed.

2. The following shows the Routing Topology page with information about the Managed Server:

With Topology Viewer, you can also:

- Choose how to group the routing. From the View By menu, you can choose to group by Middleware, host, or application.
- Show or hide the filters.
- View the targets by status. Click the green up arrow or the red down arrow at the top of the page. A list of the targets with the specified status is shown.
- Search for a target within the topology. This makes it easier to find a target if you have many targets. Click the **Toggle Find Toolbar**. Then, enter the name, type, of status, and click **Find**.

The Find results box is displayed. Click the target name to highlight the target. The topology is repositioned so you can see the target if it was not previously visible in the viewing area.

- Hide or show the status or metrics. From **Options**, click **Annotations**, then **Status**, **Metrics**, **Metric Names and Values**, or **No Metrics**.

If you select Metrics or Metric Names and Values, one or more key performance metrics for the component are displayed. (You cannot change the metrics that are displayed.)

- Reposition the topology and change its orientation:
 - To change the orientation, from the Options menu, choose **Layout**, then **Left to Right** or **Top Down**.
 - To reposition the topology, click in the topology, but not on a target or route. Drag the topology to position it.
 - To change what is visible in the topology view, click the arrow in the right-hand bottom corner. Then, drag the shaded section in the navigator window, which is located in the bottom right.
- Navigate to the home page of a target. Right-click the target, and select **Home**.
- Perform operations directly on the target by right-clicking. The right-click target menu is displayed. For example, from this menu, you can start or stop an Oracle WebLogic Server or view additional performance metrics.
- View the routing relationships between components. For example, you can view the routing from Oracle HTTP Server to Oracle WebLogic Server. Clicking on the line between the two targets displays the URLs used.

Managing Log Files and Diagnostic Data

Oracle Fusion Middleware components generate log files containing messages that record all types of events, including startup and shutdown information, errors, warning messages, and access information on HTTP requests. This chapter describes how to find information about the cause of an error and its corrective action and to view and manage log files to assist in monitoring system activity and in diagnosing problems.

It contains the following sections:

- [Section 12.1, "Overview of Oracle Fusion Middleware Logging"](#)
- [Section 12.2, "Understanding ODL Messages and ODL Log Files"](#)
- [Section 12.3, "Viewing and Searching Log Files"](#)
- [Section 12.4, "Configuring Settings for Log Files"](#)
- [Section 12.5, "Correlating Messages Across Log Files and Components"](#)
- [Section 12.6, "Configuring Tracing"](#)

12.1 Overview of Oracle Fusion Middleware Logging

The following topics describe HTTP access logging and diagnostic logging.

- [Understanding Oracle Fusion Middleware HTTP Access Logging](#)
- [Understanding Oracle Fusion Middleware Diagnostic Logging](#)

12.1.1 Understanding Oracle Fusion Middleware HTTP Access Logging

By default, Oracle WebLogic Server is configured to use the common log format for HTTP access logs. Oracle WebLogic Server also supports the extended log format, an emerging standard defined by the draft specification from the World Wide Web Consortium (W3C).

When you install Oracle WebLogic Server with Oracle JRF, it uses the extended log format for HTTP access logs by default. The extended log format allows you to specify the type and order of information recorded about each HTTP communication.

Oracle Fusion Middleware supports the following field identifiers:

- **date:** The date at which transaction completed. The field has the format YYYY-MM-DD. All dates are specified in GMT.
- **time:** The time at which transaction completed. The field has the format HH:MM, HH:MM:SS or HH:MM:SS.S where HH is the hour in 24 hour format, MM is minutes and SS is seconds. All times are specified in GMT.

- `cs-method`: The request method, for example GET or POST. This field has type `<name>`, as defined in the W3C specification.
- `cs-url`: The full requested URI. This field has type `<uri>`, as defined in the W3C specification.
- `ctx-ecid`: The Execution Context ID (ECID). The ECID is a globally unique identifier associated with the execution of a particular request.
- `ctx-rid`: The Relationship ID (RID). The RID distinguishes the work done in one thread on one process, from work done by any other threads on this and other processes on behalf of the same request.
- `sc-status`: The status code of the response, for example (404) indicating a "File not found" status. This field has type `<integer>`, as defined in the W3C specification.

For information about the extended log format fields, see:

<http://www.w3.org/TR/WD-logfile.html>

12.1.2 Understanding Oracle Fusion Middleware Diagnostic Logging

Most Oracle Fusion Middleware components write diagnostic log files in the **Oracle Diagnostic Logging** (ODL) format. Log file naming and the format of the contents of log files conforms to an Oracle standard. By default, the diagnostic messages are written in text format.

ODL provides the following benefits:

- The capability to limit the total amount of diagnostic information saved. You can set the level of information saved and you can specify the maximum size of the log file and the log file directory.
- When you reach the specified size, older segment files are removed and newer segment files are saved in chronological fashion.
- Components can remain active, and do not need to be shutdown, when older diagnostic logging files are deleted.

You can view log files using Fusion Middleware Control or the WLST `displayLogs` command, or you can download log files to your local client and view them using another tool (for example, a text editor or another file viewing utility).

Note: Oracle WebLogic Server does not use the ODL format. For information about the Oracle WebLogic Server log format, see *Configuring Log Files and Filtering Log Messages for Oracle WebLogic Server*.

12.2 Understanding ODL Messages and ODL Log Files

Using ODL, diagnostic messages are written to log files and each message includes information, such as the time, component ID, and user.

The following example shows an ODL format error messages from Oracle HTTP Server:

```
[2014-03-13T12:31:29.0584-07:00] [OHS] [NOTIFICATION:16] [OHS-9999]
[mod_weblogic.c] [host_id: example] [host_addr: nn.nnn.nn.nn] [pid: 12789]
[tid: 46919953675776] [user: username VirtualHost: main]
WebLogic Server Plugin version 12.1.2 <WLSPLUGINS_MAIN_LINUX.X64_130502.1731>
```

In the message, the fields map to the following attributes, which are described in [Table 12-1](#):

- Timestamp, originating: 2014-03-13T12:31:29.0584-07:00
- Organization ID: OHS
- Message Type: NOTIFICATION:16
- Component ID: mod_weblogic.c
- Host ID: host_id: example
- Host Address: host_addr: nn.nnn.nn.nn
- Process ID: pid: 12789
- Thread ID: tid: 46919953675776
- User ID: userId: username
- Virtual Host: *VirtualHost: main*
- Message Text: "WebLogic Server Plugin version 12.1.2
<WLSPLUGINS_MAIN_LINUX.X64_130502.1731>"

By default, the information is written to the log files in ODL text format. You can change the format to ODL XML format, as described in [Section 12.4.4](#).

[Table 12-1](#) describes the contents of an ODL message. For any given component, the optional attributes may not be present in the generated diagnostic messages.

Table 12-1 ODL Format Message Fields

Attribute Name	Description	Required
Timestamp, Originating (TIME)	The date and time when the message was generated. This reflects the local time zone.	Yes
Timestamp, normalized (time_norm)	The timestamp normalized for clock drift across hosts. This field is used when the diagnostic message is copied to a repository on a different host.	No
Organization ID (org_id)	The organization ID for the originating component.	No
INSTANCE_ID (INST_ID)	The name of the instance to which the component that originated the message belongs.	No
COMPONENT ID (COMP_ID)	The ID of the component that originated the message.	Yes
MESSAGE_ID (MSG_ID)	The ID that uniquely identifies the message within the component. The ID consists of a prefix that represents the component, followed by a dash, then a 5-digit number. For example: OHS-51009	Yes
MESSAGE_TYPE (MSG_TYPE)	The type of message. Possible values are: INCIDENT_ERROR, ERROR, WARNING, NOTIFICATION, TRACE, and UNKNOWN. See Table 12-3 for information about the message types.	Yes
MESSAGE_LEVEL (MSG_LEVEL)	The message level, represented by an integer value that qualifies the message type. Possible values are from 1 (highest severity) through 32 (lowest severity). See Table 12-3 for information about the message levels.	Yes
HOST_ID (HOST_ID)	The name of the host where the message originated.	No
HOST_NW_ADDR (HOST_ADDR)	The network address of the host where the message originated.	No
MODULE_ID (MODULE)	The ID of the module that originated the message. If the component is a single module, the component ID is listed for this attribute.	Yes

Table 12–1 (Cont.) ODL Format Message Fields

Attribute Name	Description	Required
PROCESS_ID (PID)	The process ID for the process or execution unit associated with the message.	No
THREAD_ID (TID)	The ID of the thread that generated the message.	No
USER_ID (USER)	The name of the user whose execution context generated the message.	No
ECID	The Execution Context ID (ECID), which is a global unique identifier of the execution of a particular request in which the originating component participates. You can use the ECID to correlate error messages from different components. See Section 12.5 for information about ECIDs.	Yes
RID	The relationship ID (RID), which distinguishes the work done in one thread on one process, from work done by any other threads on this and other processes, on behalf of the same request. See Section 12.5 for information about RIDs.	No
SUPPL_ATTRS	An additional list of name/value pairs which contain component-specific attributes about the event. Oracle Fusion Middleware provides the supplemental attribute DSID (Diagnostic Session ID). DSID is an ID for a user session and is used to map a set of log messages, incidents, and other diagnostic data to a user session. For example, you can see if a specific incident generated in a user session may have been preceded by earlier incidents in the same session, and could therefore be the root cause of the subsequent incident.	No
MESSAGE TEXT (TEXT)	The text of the message.	Yes
Message Arguments (arg)	A list of arguments bound with the message text.	No
Supplemental Detail	Supplemental information about the event, including more detailed information than the message text.	No

The log file location depends on the type of component:

- For most Java components, the log file location is:

(UNIX) `DOMAIN_HOME/servers/server_name/logs`
 (Windows) `DOMAIN_HOME\servers\server_name\logs`

The default name of a log file is `server-name-diagnostic.log`.

- For system components, the default log file location is:

(UNIX) `DOMAIN_HOME/servers/component_name/logs`
 (Windows) `DOMAIN_HOME\servers\component_name\logs`

[Table 12–2](#) shows the log file location for components of Oracle Fusion Middleware.

Table 12–2 Log File Location for Oracle Fusion Middleware Components

Component	Log File Location
Fusion Middleware Control	<code>DOMAIN_HOME/sysman/log/emoms.log</code> <code>DOMAIN_HOME/sysman/log/emoms.trc</code>
Oracle Application Development Framework	<code>DOMAIN_HOME/servers/server_name/logs/server-name-diagnostic.log</code>
Oracle Business Activity Monitoring	<code>DOMAIN_HOME/servers/server_name/logs/server-name-diagnostic.log</code>
Oracle Business Process Management	<code>DOMAIN_HOME/servers/server_name/logs/server-name-diagnostic.log</code>

Table 12–2 (Cont.) Log File Location for Oracle Fusion Middleware Components

Component	Log File Location
Oracle Enterprise Scheduler	<i>DOMAIN_HOME/servers/server_name/logs/server-name-diagnostic.log</i>
Oracle Event Processing	<i>DOMAIN_HOME/servers/server_name/logs/server-name-diagnostic.log</i>
Oracle HTTP Server	<i>DOMAIN_HOME/servers/component_name/logs/*.log</i>
Oracle Managed File Transfer	<i>DOMAIN_HOME/servers/server_name/logs/server-name-diagnostic.log</i>
Oracle Platform Security Services	<i>DOMAIN_HOME/servers/server_name/logs/server-name-diagnostic.log</i>
Oracle Service Bus	<i>DOMAIN_HOME/servers/server_name/logs/server-name-diagnostic.log</i>
Oracle SOA Suite	<i>DOMAIN_HOME/servers/server_name/logs/server-name-diagnostic.log</i>
Oracle TopLink	<i>DOMAIN_HOME/servers/server_name/logs/server-name-diagnostic.log</i>
Oracle Web Services Manager	<i>DOMAIN_HOME/servers/server_name/logs/owsm/msglogging</i> <i>DOMAIN_HOME/servers/server_name/logs/owsm-diagnostic.log</i>
Oracle WebLogic Server	<i>DOMAIN_HOME/servers/server_name/logs/server-name-diagnostic.log</i>
Repository Creation Utility	By default, writes to file specified in RCU_LOG_LOCATION. If not specified, attempts to write to the following locations: <ol style="list-style-type: none"> <i>ORACLE_HOME/rcu/log/timestamp</i> <i>/tmp/logdir.timestamp</i>

12.3 Viewing and Searching Log Files

You can view, list, and search log files across Oracle Fusion Middleware components. You can view and search log files using Fusion Middleware Control or you can download a log file to your local client and view the log files using another tool. You can also list, view, and search log files using the WLST command-line tool.

This section covers the following topics:

- [Viewing Log Files and Their Messages](#)
- [Searching Log Files](#)
- [Downloading Log Files](#)

Note the following about using the WLST commands to view the log files:

- To use the custom WLST logging commands, you must invoke the WLST script from the Oracle Common home. See [Section 2.4.2](#) for more information.
- The log viewing commands work whether you are connected or not connected to a WebLogic server. If you are not connected, you must specify the path in the `oracleInstance` parameter, passing it the path to the domain home.
- Most of the WLST logging commands require that you are running in the `domainRuntime` tree. For example, to connect and to run in the `domainRuntime` tree, use the following WLST commands:

```
connect('username', 'password', 'localhost:port_number')
domainRuntime()
```

For more information about the commands, see "Logging Custom WLST Commands" in the *WLST Command Reference for Infrastructure Components*.

soa_server1 ? Logged in as **weblogic** slc01fkr.us.oracle.com

WebLogic Server ▶ Start Up ▶ Shut Down... Page Refreshed **Mar 19, 2014 12:05:14 PM PDT**

/Domain_soa_domain/soa_domain/soa_server1 > Log Messages > Log Files > View Log File: soa_server1.log

View Log File: soa_server1.log View Manual Refresh

Name /scratch/oracle1/Oracle/domains/soa_domain/servers/soa_server1/logs/soa_server1.log Log Server Type Size 314.39 (KB) Download

Last Modified Mar 19, 2014 12:02:39 PM PDT

Date Range Start Date Mar 19, 2014 02:26:06 End Date Mar 19, 2014 12:03:40

View

Time	Message Type	Message ID	Message
Mar 19, 2014 2:26:06 AM PDT	Notification	BEA-001128	Connection for pool "SOADDataSource" has been closed.
Mar 19, 2014 2:26:06 AM PDT	Notification	BEA-001128	Connection for pool "SOADDataSource" has been closed.
Mar 19, 2014 2:26:07 AM PDT	Notification	BEA-000628	Created "1" resources for pool "EssInterr
Mar 19, 2014 2:26:07 AM PDT	Notification	BEA-000628	Created "1" resources for pool "SOADData
Mar 19, 2014 2:26:07 AM PDT	Notification	BEA-000628	Created "1" resources for pool "EssInterr
Mar 19, 2014 2:26:16 AM PDT	Notification	BEA-001128	Connection for pool "SOALocalTxDataSo
Mar 19, 2014 2:26:21 AM PDT	Notification	BEA-000628	Created "1" resources for pool "SOADData

Rows Selected 1 Columns Hidden 32 Total Rows : 1000

Mar 19, 2014 2:26:06 AM PDT (Notification)

Message ID	BEA-001128	Module	JDBC
Message Level	1	Host	slc01fkr
ECID	c47a6323-f17f-48b8-b8dd-630ccdf0c6d-000ed14e	Host IP Address	10.240.82.231
Relationship ID	0	User	<WLS Kernel>
Component	soa_server1	Thread ID	[ACTIVE] ExecuteThread: '8' for queue: 'weblogic.kernel.Default (self-tuning)'

Message Connection for pool "SOADDataSource" has been closed.

By default, the messages are sorted by time, in ascending order. You can sort the messages by the any of the columns, such as Message Type, by clicking the column name.

- To view messages that are related by time or ECID, click **View Related Messages** and select **by Time** or **by ECID (Execution Context ID)**.

The Related Messages page is displayed.

12.3.1.2 Viewing Log Files and Their Messages Using WLST

You can list the log files for an Oracle WebLogic Server domain, a server, or component using the WLST `listLogs` command.

You can use this command while connected or disconnected. While connected, the default target is the Oracle WebLogic Server domain.

To list the log files, first use the `domainRuntime` command as described in [Section 12.3](#). The following describes how to list and view log files:

- To list all of the log files for the Oracle WebLogic Server `wls_server_1`, use the following command:

```
listLogs(target='wls_server_1')
file://slc01fkr/scratch/oracle1/Oracle/domains/base_domain/servers/wls_server_1/logs/wls_server_1.log
2014-03-21 06:55:37          500.1K wls_server_1.log00026
2014-03-21 07:49:08          500.1K wls_server_1.log00027
2014-03-21 08:46:29          500.4K wls_server_1.log00028
2014-03-21 09:45:29          500.4K wls_server_1.log00029
```



```

2014-03-21 10:43:00          500.3K wls_server_1.log00030
2014-03-21 11:39:56          500.3K wls_server_1.log00031
2014-03-21 12:38:56          500.4K wls_server_1.log00032
2014-03-21 13:18:06          358.1K wls_server_1.log

file://slc01fkr/scratch/oracle1/Oracle/domains/base_domain/servers/wls_server_
1/logs/wls_server_1.out
2014-03-13 11:00:05          4M wls_server_1.out00001
2014-03-21 13:18:06          12.1M wls_server_1.out
...

```

- To list the logs for a system component, use one of the following formats:

```

listLogs(target='component_name')
listLogs(target='sc:component_name')

```

For example, to list the logs for the Oracle HTTP Server ohs1, use the following command:

```
listLogs(target='ohs1')
```

- To list the logs while disconnected, you must specify the `oracleInstance` parameter, passing it the path of the domain. For example, to list the log files for the Managed Server `wls_server_1`:

```
listLogs(oracleInstance='/scratch/Oracle/config/domains/WLS_domain',
        target='wls_server_1')
```

- To view the diagnostic messages in log files, use the `WLST displayLogs` command. This command works when you are either connected or disconnected.

For example, to view the messages generated in the last 10 minutes in the log files for the Oracle WebLogic Server domain, use the following command:

```
displayLogs(last=10)
```

```

[2014-03-21T13:30:11.892-07:00] [wls_server_1] [WARNING] [WSM-09004]
 [oracle.wsm.resources.common] [host: slc01fkr] [nwaddr: 10.240.82.231]
[tid: [ACTIVE].ExecuteThread: '5' for queue: 'weblogic.kernel.Default
(self-tuning)'] [userId: OracleSystemUser]
[ecid: 66217af9-247f-4344-94a9-14f90e75a586-00070b85,0] [APP: wsm-pm] [TARGET:
/base_domain/wls_server_1/wsm-pm]
[LOG_FILE: /scratch/oracle1/Oracle/domains/base_domain/servers/wls_server_
1/logs/wls_server_1-diagnostic.log]
Component auditing cannot be initialized.
[2014-03-21T13:30:11.895-07:00] [wls_server_1] [NOTIFICATION] [BEA-010227]
 [EJB] [host: slc01fkr] [nwaddr: 10.240.82.231] [tid: [ACTIVE].ExecuteThread:
 '5' for queue: 'weblogic.kernel.Default (self-tuning)']
[userId: OracleSystemUser]
[ecid: 66217af9-247f-4344-94a9-14f90e75a586-00070b85,0] [TXN_ID:
BEA1-7438ECB7CDFCAF163A9A]
[TARGET: /base_domain/wls_server_1]
[LOG_FILE: /scratch/oracle1/Oracle/domains/base_domain/servers/wls_server_
1/logs/wls_server_1.log]
EJB exception occurred during invocation from home or business:
 weblogic.ejb.container.internal.StatelessEJBHomeImpl@314c2224 generated
exception: java.lang.reflect.UndeclaredThrowableException

```

The previous command returns the messages sorted by time, in ascending order.

- To display the logs for a system component, use one of the following formats:


```
listLogs(target='component_name')
listLogs(target='sc:component_name')
```

For example, to display the log files for the Oracle HTTP Server ohs_1, use the following command:

```
displayLogs(target='sc:ohs_1')
```

You can search the messages by specifying particular criteria and sort the output, as described in [Section 12.3.2](#).

See "Logging Custom WLST Commands" in the *WLST Command Reference for Infrastructure Components* for more information about the `listLogs` and `displayLogs` commands.

12.3.2 Searching Log Files

You can search for diagnostic messages by time, type of message, and certain log file attributes by using Fusion Middleware Control or WLST commands, as described in the following topics:

- [Searching Log Files Using Fusion Middleware Control](#)
- [Searching Log Files Using WLST](#)

12.3.2.1 Searching Log Files Using Fusion Middleware Control

You can search for diagnostic messages using standard and supplemental ODL attributes using the Log Messages page of Fusion Middleware Control. By default, this page shows a summary of the logged issues for the last hour.

You can modify the search criteria to identify messages of relevance. You can view the search results in different modes, allowing ease of navigation through large amounts of data.

The following sections describe how to search log files:

- [Searching Log Files: Basic Searches](#)
- [Searching Log Files: Advanced Searches](#)

12.3.2.1.1 Searching Log Files: Basic Searches This section describes how to perform basic searches for log messages.

You can search for all of the messages for all of the entities in a domain, an Oracle WebLogic Server, a component, or an application.

For example, to search for messages for a domain:

1. From the WebLogic Domain menu, choose **Logs**, then **View Log Messages**.
To search for messages for a component or application, select the component or application. Then choose **Logs**, then **View Log Messages** from that target's menu.
The Log Messages page displays a Search section and a table that shows a summary of the messages for the 10 minutes.
2. In the Date Range section, you can select either:
 - **Most Recent:** If you select this option, select a time, such as 3 hours. The default is 10 minutes.

- **Time Interval:** If you select this option, select the calendar icon for **Start Date**. Select a date and time. Then, select the calendar icon for **End Date**. Select a date and time.
3. In the Message Types section, select one or more of the message types. The types are described in [Table 12-3](#).
 4. You can specify more search criteria, as described in [Section 12.3.2.1.2](#).
 5. Click **Search**. The results are shown, as in the following figure:

soa_server2 Logged in as weblogic

WebLogic Server Start Up Shut Down... Page Refreshed Mar 19, 2014 12:09:00 PM PDT

/Domain_soa_domain/soa_domain/soa_server2 > Log Messages

Log Messages Target Log Files... Manual Refresh

Search

Selected Targets (33)

Date Range: Most Recent 10 Days

* Message Types: Incident Error Error Warning Notification Trace Unknown

* Search: Selected Fields All Fields

Search

Tip: Enter one or more keywords separated by a comma. If keyword contains comma then prepend the comma with '\'. Example: weblogic, server\, weblogic server will search.

Time	Message Type	Message ID	Message
Mar 14, 2014 10:53:04 AM PDT	Warning		Detected that sensors created in an invalid ADP...
Mar 14, 2014 10:53:09 AM PDT	Warning	BEA-002919	Unable to find a Work Manager with name wm/Sir...
Mar 14, 2014 10:53:10 AM PDT	Warning	BEA-000000	2014-03-14 10:53:10.769/304.698 Oracle Coherer...
Mar 14, 2014 10:54:06 AM PDT	Warning	BEA-050006	An attempt was made to look up the versioned ob...
Mar 14, 2014 10:54:09 AM PDT	Warning		Failed to validate the xml content. Reason: cvc-cor...
Mar 14, 2014 10:54:09 AM PDT	Warning	BEA-000000	Failed to validate the xml content. Reason: cvc-cor...

6. To help identify messages of relevance, in the table, for **Show**, select one of the following modes:
 - **Messages:** Shows the matching messages.

To see the details of a particular message, click the message. The details are displayed below the table of messages.

To view related messages, select a message, then click **View Related Messages** and select **by Time** or **by ECID (Execution Context ID)**.
 - **Group by:** You can choose to group by one of the selections. This option groups the messages based on the criteria you selected, such as Message Type or ECID.

To see the messages, click the count in one of the message type columns. The Messages by Message Type page is displayed. To see the details of a particular message, click the message. The details are displayed below the table of messages.

12.3.2.1.2 Searching Log Files: Advanced Searches You can refine your search criteria using the following controls in the Log Messages page:

- **Message:** Select an operator, such as **contains** and then enter a value to be matched.

- **Add Fields:** Click this to specify additional criteria, such as Host, which lets you narrow the search to particular hosts. Then click **Add**.
For each field you add, select an operator, such as **contains** and then enter a value to be matched.
- **Selected Targets:** Expand this to see the targets that are participating in the search. To add targets, click **Add** and provide information in the dialog box. To remove targets, select the target and click **Remove**.

12.3.2.2 Searching Log Files Using WLST

You can search the log files using the WLST `displayLogs` command. You can narrow your search by specifying criteria, such as time, component ID, message type, or ECID. For example:

- To search for error messages generated in the last 5 minutes, for a system component such as the Oracle HTTP Server `ohs1`, use the following command:

```
displayLogs(target='sc:ohs1', last=5)
```

- To search for error messages generated in the last 10 minutes for the Managed Server `wls_server_1`, use the following command:

```
displayLogs(oracleInstance='/scratch/Oracle/config/domains/WLS_domain',
target='wls_server_1', last=10)
```

You can narrow your search by using the `query` parameter and specifying criteria, such as component ID, message type, or ECID. In the `query` clause, you can specify a query expression with any of the attributes listed in [Table 12-1](#). Some of the criteria you can use are:

- Types of messages. For example, to search for `ERROR` and `INCIDENT_ERROR` messages for the Managed Server `wls_server_1`, use the following command:

```
displayLogs(oracleInstance='/scratch/Oracle/config/domains/wls_domain',
target='wls_server_1',
query='MSG_TYPE eq ERROR or MSG_TYPE eq INCIDENT_ERROR')
```

- A particular ECID. For example, to search for error messages with a particular ECID (`0000I3K7DCnAhKB5JZ4Eyf19wAgN000001,0`) for the Managed Server `wls_server_1`, use the following command:

```
displayLogs(oracleInstance='/scratch/Oracle/config/domains/wls_domain',
target='wls_server_1',
query='ecid eq 0000I3K7DCnAhKB5JZ4Eyf19wAgN000001,0')
```

- Component type. For example, to search for messages from Oracle HTTP Server instances, use the following query:

```
displayLogs(query='COMPONENT_ID eq ohs')
```

- Range of time. To search for error messages that occurred within a specified range of time, you specify the attribute `TSTZ_ORIGINATING` with both `from` and `to` operators, using the following format:

```
displayLogs(query='TSTZ_ORIGINATING from start_time and
TSTZ_ORIGINATING to end_time')
```

You specify the date using the following ISO 8601 time format:

```
YYYY-MM-DDThh:mm:ss-hh:mm_offset_from_UTC
```

For example:

```
2014-03-30T12:00:00-08:00
```

For example, to display the error message from between 8:00 a.m. and 11 a.m. on March 17, 2014, use the following command:

```
displayLogs (query='TSTZ_ORIGINATING from 2014-03-17T08:00:00-07:00
and TSTZ_ORIGINATING to 2014-03-17T11:00:00-07:00')
```

- **Group messages.** To display a count of messages, grouped by specific attributes, use the `groupBy` parameter to the WLST command `displayLogs`. For example, to display the count of WARNING messages by component, use the following command:

```
displayLogs (groupBy=['COMPONENT_ID'], query='MSG_TYPE eq WARNING')
```

- **Group messages by supplemental attributes.** If you use the DMS event tracing commands, you can create a destination that enables you to query and group messages by specific supplemental attributes. In this case, you use the `addDMSEventDestination` command to create a destination with the property `writeDataAsMessageAttributes`. (See "addDMSEventDestination" in the *WLST Command Reference for Infrastructure Components*.)

Then, you can query the log messages. For example, to query by Completing Party:

```
displayLogs (log="DOMAIN_
HOME/servers/AdminServer/logs/DMSEventTraceLoggerDestination-event.log",
groupBy=["SUPPL_ATTR.dms.NounType",
"SUPPL_ATTR.dms.NounPath",
"SUPPL_ATTR.org.service.CompletingParty"])
```

This command returns the following:

```
-----+-----+-----+-----+-----+
-
dms.NounType      | dms.NounPath      | org.service.CompletingParty | COUNT
-----+-----+-----+-----+-----+
CallCenter_Agent  | /callAgent/Freya  | null                        | 25
CallCenter_Agent  | /callAgent/Johann | null                        | 20
CallCenter_Agent  | /callAgent/Rhys   | null                        | 25
CallCenter_City   | /callCenter/fr/Pau| null                        | 2
CallCenter_City   | /callCenter/fr/Vichy| null                       | 2
CallCenter_City   | /callCenter/uk/Watford| null                       | 2
CallCenter_Country| /callCenter/de    | null                        | 6
CallCenter_Country| /callCenter/fr    | null                        | 6
CallCenter_Country| /callCenter/uk    | null                        | 6
CallCenter_IncomingCall| /callCenter/fr/Pau/inCalls| agent                       | 10
CallCenter_IncomingCall| /callCenter/fr/Pau/inCalls| caller                       | 40
```

12.3.3 Downloading Log Files

You can download messages using Fusion Middleware Control or WLST commands, as described in the following topics:

- [Downloading Log Files Using Fusion Middleware Control](#)
- [Downloading Log Files for Specific Components Using Fusion Middleware Control](#)
- [Downloading Specific Types of Messages Using Fusion Middleware Control](#)

- [Downloading Log Files Using WLST](#)

12.3.3.1 Downloading Log Files Using Fusion Middleware Control

You can download the log messages to a file. You can download either the matching messages from a search or the messages in a particular log file.

To download the matching messages from a search to a file using Fusion Middleware Control:

1. From the navigation pane, expand the domain and select the target, for example by clicking on the domain.
2. From the dynamic target menu, such as the WebLogic Domain menu, choose **Logs**, then **View Log Messages**.

The Log Messages page is displayed.

3. Search for particular types of messages as described in [Section 12.3.2.1](#).
4. Select a file type by clicking **Export Messages to File** and select one of the following:
 - **As Oracle Diagnostic Log Text (.txt)**
 - **As Oracle Diagnostic Log Text (.xml)**
 - **As Comma-Separated List (.csv)**

An Opening dialog box is displayed.

5. Select either **Open With** or **Save to Disk**. Click **OK**.

12.3.3.2 Downloading Log Files for Specific Components Using Fusion Middleware Control

To download the log files for a specific component using Fusion Middleware Control:

1. For system components, from the navigation pane, expand the installation type, such as **HTTP Server** and select the component. For Java components, from the navigation pane, expand the component type, and then select the component.
2. From the dynamic target menu, choose **Logs**, then **View Log Messages**.

The Log Messages page is displayed.

3. Click **Target Log Files**.

The Log Files page is displayed. On this page, you can see a list of log files related to the component or application.

4. Select a log file and click **Download**.
5. An Opening dialog box is displayed.
6. Select either **Open With** or **Save to Disk**. Click **OK**.

12.3.3.3 Downloading Specific Types of Messages Using Fusion Middleware Control

To export specific types of messages or messages with a particular Message ID to a file:

1. From the navigation pane, expand the domain and select a target.
2. From the dynamic target menu, choose **Logs**, then **View Log Messages**.

The Log Messages page is displayed.

3. Search for particular types of messages as described in [Section 12.3.2.1](#).
4. For **Show**, select **Group by Message Type** or **Group by Message ID**.
5. To download the messages into a file, if you selected **Group by Message Type**, select the link in one of the columns that lists the number of messages, such as the **Errors** column. If you selected **Group by Message ID**, select one of the links in the **Occurrences** column.

The **Messages by Message Type** page or **Message by Message ID** is displayed.

6. Select a file type by clicking **Export Messages to File** and select one of the following:
 - **As Oracle Diagnostic Log Text (.txt)**
 - **As Oracle Diagnostic Log Text (.xml)**
 - **As Comma-Separated List (.csv)**

An Opening dialog box is displayed.

7. Select either **Open With** or **Save to Disk**. Click **OK**.

12.3.3.4 Downloading Log Files Using WLST

You can download log files using the WLST `displayLogs` command and redirecting the output to a file. For example:

```
displayLogs(type=['ERROR','INCIDENT_ERROR'], exportFile='/scratch/tmp/download_log.txt')
```

The messages are written to the file `download_log.txt` in the specified directory. By default, they are written to standard output.

12.4 Configuring Settings for Log Files

You can change the log settings of Managed Servers and Java components using Fusion Middleware Control or WLST.

Note: For many system components, which are listed in [Section 2.4.3](#), you cannot configure settings for log files using Fusion Middleware Control. For information about how to configure options for log files for system components, see the administrator's guide for the component.

For Java components, you can configure the names and locations of log files, the size of the log files, the level of information written to the log files, the format, and the Locale encoding, as described in the following topics:

- [Changing Log File Locations](#)
- [Configuring Log File Rotation](#)
- [Setting the Level of Information Written to Log Files](#)
- [Specifying the Log File Format](#)
- [Specifying the Log File Locale](#)

Note the following about using the WLST commands to configure log settings:

- To use the custom WLST logging commands, you must invoke the WLST script from the Oracle Common home. See [Section 2.4.2](#) for more information.
- The configuration commands, such as `setLogLevel`, only work in connected mode. That is, you must connect to a running WebLogic Server instance before you invoke the commands.

The configuration commands are supported for Java components that run within a WebLogic Server, but are not supported for Oracle WebLogic Server. The configuration commands are not supported for system components.

- Most of the WLST logging commands require that you are running in the `domainRuntime` tree. For example, to connect and to run in the `domainRuntime` tree, use the following commands:

```
connect('username', 'password', 'localhost:port_number')
domainRuntime()
```

- The `listLoggers`, `getLogLevel`, and `setLogLevel` commands work in `config` and `runtime` mode. In `config` mode the commands work on loggers that are defined in the configuration file. In `runtime` mode, the commands work directly with loggers that are defined in the server JVM. By default, the `setLogLevel` command sets the level on the run-time logger and updates the logger definition in the configuration file. By default, the `listLoggers` and `getLogLevel` commands return run-time loggers.

For more information about the commands, see "Logging Custom WLST Commands" in the *WLST Command Reference for Infrastructure Components*.

12.4.1 Changing Log File Locations

You can change the name and location of log files by using Fusion Middleware Control or WLST commands, as described in the following topics:

- [Changing Log File Locations Using Fusion Middleware Control](#)
- [Changing Log File Locations Using WLST](#)

12.4.1.1 Changing Log File Locations Using Fusion Middleware Control

To change the name and location of a component log file using Fusion Middleware Control:

1. From the navigation pane, select the component.
2. From the dynamic target menu, choose **Logs**, then **Log Configuration**.

The Log Configuration page is displayed.

Note that the navigation may be different for some components. For example, for Oracle HTTP Server, you choose **Administration**, then **Log Configuration**.

3. Select the Log Files tab.
4. In the table, select the log handler and click **Edit Configuration**.

The Edit Log File dialog box is displayed, as shown in the following figure:

5. For **Log Path**, enter a new path.
6. Click **OK**.
7. In the confirmation window, click **Close**.

Note that if you change the location of Oracle HTTP Server log files, the location of the `access_log` and `ohsn.log` files are changed, but the location of `console~OHS~1.log` is not changed.

12.4.1.2 Changing Log File Locations Using WLST

To change the log file location using WLST, use the `configureLogHandler` command. For example, to change the path of the logger named `odl-handler`, use the following command:

```
configureLogHandler(name='odl-handler', path='/scratch/Oracle/logs')
```

12.4.2 Configuring Log File Rotation

bug 8520773: to change to xml, must be named `log.xml`. In EM, don't specify file name and `log.xml` will be created.

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 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:

- [Specifying Log File Rotation Using Fusion Middleware Control](#)
- [Specifying Log File Rotation Using WLST](#)

12.4.2.1 Specifying Log File Rotation Using Fusion Middleware Control

To configure log file rotation using Fusion Middleware Control:

1. From the navigation pane, select the component.
2. From the dynamic target menu, choose **Logs**, then **Log Configuration**.

The Log Configuration page is displayed.

Note that the navigation may be different for some components. For example, for Oracle HTTP Server, you choose **Administration**, then **Log Configuration**.

3. Select the Log Files tab.
4. In the table, select the logger and click **Edit Configuration**.
The Edit Log File dialog box is displayed.
5. 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**, click the calendar and select the date and time when you want the rotation to start. For example, select September 8, 2010 6:00 AM.
 - 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.

6. Click **OK**.

7. In the confirmation window, click **Close**.

12.4.2.2 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 5 MB and rotates when it reaches that size, use the following command:

```
configureLogHandler(name='odl-handler', maxFileSize='5M')
```

12.4.3 Setting the Level of Information Written to Log Files

You can configure the amount and type of information written to log files by specifying the message type and level. For each message type, possible values for the message level are from 1 (lowest severity) through 32 (highest severity). Some components support only some of the levels for each message type. See the administrator's guide for your component for more information. Generally, you need to specify only the type; you do not need to specify the level.

When you specify the type, Oracle Fusion Middleware returns all messages of that type, as well as the messages that have a higher severity. For example, if you set the message type to `WARNING`, Oracle Fusion Middleware also returns messages of type `INCIDENT_ERROR` and `ERROR`.

[Table 12–3](#) describes the message types and the most common levels for each type.

Table 12–3 Diagnostic Message Types and Level

Message Type	Level	Description
INCIDENT_ERROR	1	A serious problem that may be caused by a bug in the product and that should be reported to Oracle Support. Examples are errors from which you cannot recover or serious problems.
ERROR	1	A serious problem that requires immediate attention from the administrator and is not caused by a bug in the product. An example is if Oracle Fusion Middleware cannot process a log file, but you can correct the problem by fixing the permissions on the document.
WARNING	1	A potential problem that should be reviewed by the administrator. Examples are invalid parameter values or a specified file does not exist.
NOTIFICATION	1	A major lifecycle event such as the activation or deactivation of a primary sub-component or feature. This is the default level for NOTIFICATION.
NOTIFICATION	16	A finer level of granularity for reporting normal events.
TRACE	1	Trace or debug information for events that are meaningful to administrators, such as public API entry or exit points.

Table 12–3 (Cont.) Diagnostic Message Types and Level

Message Type	Level	Description
TRACE	16	Detailed trace or debug information that can help Oracle Support diagnose problems with a particular subsystem.
TRACE	32	Very detailed trace or debug information that can help Oracle Support diagnose problems with a particular subsystem.

The default is NOTIFICATION, level 1.

The INCIDENT_ERROR, ERROR, WARNING, and NOTIFICATION with level 1 have no performance impact. For other types and levels, note the following:

- NOTIFICATION, with level 16: Minimal performance impact.
- TRACE, with level 1: Small performance impact. You can enable this level occasionally on a production environment to debug problems.
- TRACE, with level 16: High performance impact. This level should not be enabled on a production environment, except on special situations to debug problems.
- TRACE, with level 32: Very high performance impact. This level should not be enabled in a production environment. It is intended to be used to debug the product on a test or development environment.

Table 12–4 shows the log level mappings among ODL format, Oracle WebLogic Server, and Java.

Table 12–4 Mapping of Log Levels Among ODL, Oracle WebLogic Server, and Java

ODL	WebLogic Server	Java
OFF	OFF	2147483647 - OFF
INCIDENT_ERROR:1	(EMERGENCY)	1100
INCIDENT_ERROR:4	EMERGENCY	1090
INCIDENT_ERROR:14	ALERT	1060
INCIDENT_ERROR:24	CRITICAL	1030
ERROR:1	(ERROR)	1000 - SEVERE
ERROR:7	ERROR	980
WARNING:1	WARNING	900 - WARNING
WARNING:7	NOTICE	880
NOTIFICATION:1	INFO	800 - INFO
NOTIFICATION:16	(DEBUG)	700 - CONFIG
TRACE:1	(DEBUG)	500 - FINE
TRACE:1	DEBUG	495
TRACE:16	(TRACE)	400 - FINER
TRACE:32	(TRACE)	300 - FINEST
TRACE:32	TRACE	295

You can configure the message levels using Fusion Middleware Control or WLST commands, as described in the following topics:

- [Configuring Message Levels Using Fusion Middleware Control](#)
- [Configuring Message Levels Using WLST](#)

12.4.3.1 Configuring Message Levels Using Fusion Middleware Control

You can set the message level for a particular log file or for loggers.

To set the message level for a component log file:

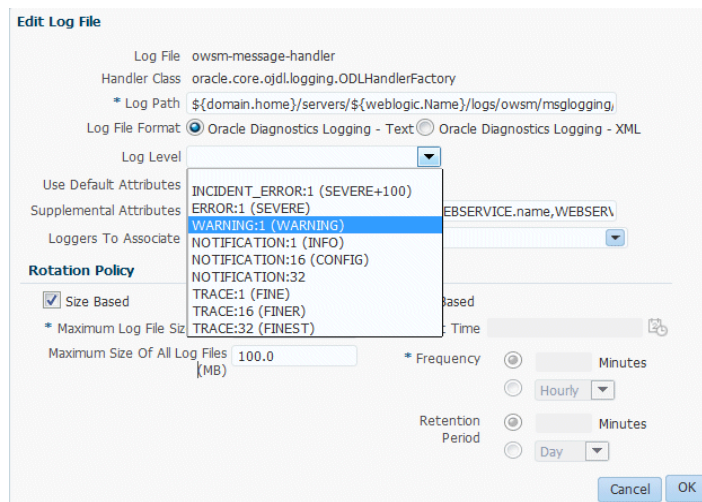
1. From the navigation pane, select the component.
2. From the dynamic target menu, choose **Logs**, then **Log Configuration**.

The Log Configuration page is displayed.

Note that the navigation may be different for some components. For example, for Oracle HTTP Server, you choose **Administration**, then **Log Configuration**.

3. Select the Log Files tab.
4. In the table, select the log file and click **Edit Configuration**.

The Edit Log File dialog box is displayed, as shown in the following figure:



5. For **Log Level**, select the logging level. For example, select **WARNING:1 (WARNING)**.
6. Click **OK**.
7. In the confirmation window, click **Close**.

To set the message level for one or more loggers for a component:

1. From the navigation pane, select the component.
2. From the dynamic target menu, choose **Logs**, then **Log Configuration**.

The Log Configuration page is displayed.

Note that the navigation may be different for some components. For example, for Oracle HTTP Server, you choose **Administration**, then **Log Configuration**.

3. Select the **Log Levels** tab.
4. For **View**, select **Runtime Loggers** or **Loggers with Persistent Log Level State**.

Run-time loggers are loggers that are currently active. Persistent loggers are loggers that are saved in a configuration file and the log levels of these loggers are

persistent across component restarts. A run-time logger can also be a persistent logger, but not all run-time loggers are persistent loggers.

5. In the table, to specify the same level for all loggers, select the logging level for the top-level logger. Then, for child loggers that do not specify that the logging level is inherited from the parent, specify **Inherited from Parent**. For most situations, that is sufficient.

However, if you need to specify the level for a particular logger, expand the logger and then, for the logger that you want to modify, select the logging level. For example, for the logger `oracle.wsm.management.logging`, select **WARNING:1 (WARNING)**.

6. Click **Apply**.

12.4.3.2 Configuring Message Levels Using WLST

To set the message level with WLST, you use the `setLogLevel` command. To get the current message level, you use the `getLogLevel` command. You must be connected to WebLogic Server before you use the configuration commands.

You can view the log level for a logger for an Oracle WebLogic Server. For example, to view the log level of the Oracle WebLogic Server `wls_server_1`, use the following command:

```
getLogLevel(logger='oracle', target='wls_server_1')
```

```
NOTIFICATION:1
```

You can set the log level for a particular logger. The following example sets the message type to `WARNING` for the logger `oracle.wsm.msg.logging`:

```
setLogLevel(target='wls_server_1', logger='oracle.wsm.msg.logging',
level='WARNING')
```

To get a list of loggers for the Oracle WebLogic Server `wls_server_1`, use the `listLoggers` command:

```
listLoggers(target='wls_server_1')
.
.
.
oracle.wsm.msg.logging | NOTIFICATION:1
oracle.wsm.nobehavior.model.NoBehaviorAssertion | <Inherited>
oracle.wsm.policy.advertisement.AdvertisementContext | <Inherited>
oracle.wsm.policy.model.impl.AndCompositeAssertion | <Inherited>
.
.
.
```

You can also filter logger names using the `pattern` parameter and a regular expression. For example, to return all loggers that begin with `oracle` in the Oracle WebLogic Server `wls_server_1`, use the following command:

```
listLoggers(target='wls_server_1', pattern='oracle.*')
```

```
-----
Logger | Level
-----
oracle | NOTIFICATION:1
 oracle.adf | <Inherited>
 oracle.adf.controller | <Inherited>
```

oracle.adf.desktopintegration	<Inherited>
oracle.adf.faces	<Inherited>

12.4.4 Specifying the Log File Format

By default, information is written to log files in ODL text format. You can change the format to ODL XML format using Fusion Middleware Control or WLST commands, as described in the following topics:

- [Specifying the Log File Format Using Fusion Middleware Control](#)
- [Specifying the Log File Format Using WLST](#)

12.4.4.1 Specifying the Log File Format Using Fusion Middleware Control

To change the format using Fusion Middleware Control:

1. From the navigation pane, select the component.
2. From the dynamic target menu, choose **Logs**, then **Log Configuration**.

The Log Configuration page is displayed.

Note that the navigation may be different for some components. For example, for Oracle HTTP Server, you choose **Administration**, then **Log Configuration**.

3. Select the Log Files tab.
4. In the table, select the log file and click **Edit Configuration**.
The Edit Log File dialog box is displayed.
5. For Log File Format, select **Oracle Diagnostics Logging - Text** or **Oracle Diagnostics Logging - XML**.
6. Click **OK**.
7. In the confirmation window, click **Close**.

12.4.4.2 Specifying the Log File Format Using WLST

To specify the log file format using WLST, you use the `configureLogHandler` command, with the `format` parameter and specify either ODL-Text or ODL-XML. ODL-Text is the default.

For example, to specify ODL-XML format, use the following command:

```
configureLogHandler (name='odl-handler', format='ODL-XML')
```

12.4.5 Specifying the Log File Locale

The language and data formats used in the log files are determined by the default locale of the server Java Virtual Machine (JVM). You can change them using the Language and Regional Options applet in Control Panel on Windows or the LANG and LC_ALL environment variables on a UNIX platform.

The character encoding of log files is determined by the server JVM's default character encoding or an optional configuration setting. You should choose an encoding that supports all languages used by the users, or the log file may be corrupted. By default, the log is in the server JVM's default character encoding. If you change the encoding, delete or rename old log files to prevent them from being damaged by the new logs appended in a different encoding.

For support of any language, Oracle recommends that you use Unicode UTF-8 encoding. On a UNIX operating system, setting the LANG and LC_All environment variables to a locale with the UTF-8 character set enables UTF-8 logging (for example, en_US.UTF-8 for the US locale in UTF-8 encoding).

You can specify the log file locale using WLST commands or by editing a file, as described in the following topics:

- [Specifying the Log File Encoding Using WLST](#)
- [Specifying the Log File Encoding in logging.xml](#)

12.4.5.1 Specifying the Log File Encoding Using WLST

To specify the log file encoding using WLST, use the `configureLogHandler` command. You can use the encoding parameter to specify the character set encoding.

For example, to specify UTF-8, use the following command:

```
configureLogHandler (name="odl-handler", encoding="UTF-8")
```

12.4.5.2 Specifying the Log File Encoding in logging.xml

To specify the log file encoding in the logging.xml file, use an optional encoding property to specify the character set encoding.

The logging.xml file is located in the following directory:

```
DOMAIN_HOME/config/fmwconfig/servers/server_name/
```

For example, to specify UTF-8, add the following encoding property in the log_handler element:

```
<property name='encoding' value='UTF-8' />
```

12.5 Correlating Messages Across Log Files and Components

Oracle Fusion Middleware components provide **message correlation** information for diagnostic messages. Message correlation information helps those viewing diagnostic messages to determine relationships between messages across components. Each diagnostic message contains an **Execution Context ID (ECID)** and a **Relationship ID (RID)**:

- An ECID is a globally unique identifier associated with the execution of a particular request. An ECID is generated when the request is first processed.
- A RID distinguishes the work done in one thread on one process, from work done by any other threads on this and other processes on behalf of the same request.

The ECID and RID help you to use log file entries to correlate messages from one application or across Oracle Fusion Middleware components. By searching for related messages using the message correlation information, multiple messages can be examined and the component that first generates a problem can be identified (this technique is called **first-fault component isolation**). Message correlation data can help establish a clear path for a diagnostic message across components, within which errors and related behavior can be understood.

You can use the ECID and RID to track requests as they move through Oracle Fusion Middleware.

The following shows an example of an ECID:

```
0000I3K7DCnAhKB5JZ4Eyf19wAgN000001,0
```


The RID is one or more numbers separated by a colon (:). The first RID created for a request is 0. Each time work is passed from a thread that has an ECID associated with it to another thread or process, a new RID is generated that encodes the relationship to its creator. That is, a new generation is created. Each shift in generation is represented by a colon and another number. For example, the seventh child of the third child of the creator of the request is:

0:3:7

You can view all the messages with the same ECID using the WLST `displayLogs` command. The following example searches for the ECID in the domain:

```
displayLogs (ecid='0000H19TwKUCs1T6uBi8UH181kWX000002')
```

You can also search for the ECID in a WebLogic Server instance, or a system component, by specifying it in the target option.

You can search for messages with a particular ECID on the Log Messages page in Fusion Middleware Control:

1. From the WebLogic Domain menu, choose **Logs**, then **View Log Messages**.
To search for messages for a component or application, select the component or application and then choose **Logs**, then **View Log Messages** from that target's menu.
2. Specify search criteria, as described in [Section 12.3.2.1.2](#).
3. Click **Search**.
4. Select a message, then click **View Related Messages** and select by **ECID (Execution Context ID)**.

The messages with the same ECID are displayed, as shown in the following figure:

The screenshot shows the 'soa_domain' WebLogic Domain interface. The breadcrumb path is '/Domain_soa_domain/soa_domain > Log Messages > Related Messages by ECID: c4cc4672-b118-477e-b427-cc85da2f44d4-000052f1'. The main heading is 'Related Messages by ECID: c4cc4672-b118-477e-b427-cc85da2f44d4-000052f1'. Below this, there are 'Selected Targets (73)' and a table of messages. The table has columns for Time, Message Type, Message ID, and Message. The first row is highlighted in blue and shows an 'Error' message: 'Failed to find the log query mbean. JMX call: validateTargets for t...'. Subsequent rows show 'Warning' messages: 'Invalid Remote Targets: [Target Name: /Domain_soa_domain/soa...' and 'java.lang.IllegalStateException: The expression "#{bindings.CustC...'.

Time	Message Type	Message ID	Message
Mar 20, 2014 6:52:27 AM PDT	Error		Failed to find the log query mbean. JMX call: validateTargets for t...
Mar 20, 2014 6:52:27 AM PDT	Warning		Invalid Remote Targets: [Target Name: /Domain_soa_domain/soa...
Mar 20, 2014 6:52:28 AM PDT	Warning	BEA-000000	java.lang.IllegalStateException: The expression "#{bindings.CustC...
Mar 20, 2014 6:52:28 AM PDT	Warning		java.lang.IllegalStateException: The expression "#{bindings.CustC...
Mar 20, 2014 6:52:28 AM PDT	Warning	BEA-000000	java.lang.IllegalStateException: The expression "#{bindings.CustC...
Mar 20, 2014 6:52:28 AM PDT	Warning		java.lang.IllegalStateException: The expression "#{bindings.CustC...
Mar 20, 2014 6:52:28 AM PDT	Warning	BEA-000000	java.lang.IllegalStateException: The expression "#{bindings.tgtCo...
Mar 20, 2014 6:52:28 AM PDT	Warning		java.lang.IllegalStateException: The expression "#{bindings.tgtCo...
Mar 20, 2014 6:52:28 AM PDT	Warning	BEA-000000	java.lang.IllegalStateException: The expression "#{bindings.tgtCo...
Mar 20, 2014 6:52:28 AM PDT	Warning		java.lang.IllegalStateException: The expression "#{bindings.tgtCo...

At the bottom of the table, it shows 'Rows Selected: 1', 'Columns Hidden: 36', and 'Total Rows: 26'.

5. Trace the ECID to the earliest message. (You may need to increase the scope to view the first message with the ECID.)

12.6 Configuring Tracing

Sometimes you need more information to troubleshoot a problem than it is usually recorded in the logs. One way to achieve that is to increase the level of messages logged by one or more components. For example, you can set the logging level to TRACE:1 or TRACE:32, as described in [Section 12.4.3](#), which results in more detailed messages being written to the log files. This is referred to as **tracing**.

However, this can often result in a large amount of log messages being written to the log files. Oracle Fusion Middleware provides the following mechanisms to fine-tune which messages are traced:

- QuickTrace, which provides fine-grained logging to memory
- Selective Trace, which provides fine-grained logging for a specific user or other properties of a request

The following topics provide information about how to use these mechanisms:

- [Configuring and Using QuickTrace](#)
- [Configuring and Using Selective Tracing](#)

12.6.1 Configuring and Using QuickTrace

QuickTrace provides fine-grained logging to memory. The following topics describe Quick Trace and how to enable and use it:

- [Understanding Quick Trace](#)
- [Configuring QuickTrace](#)
- [Writing Trace Messages to a File](#)
- [Disabling QuickTrace Using WLST](#)

12.6.1.1 Understanding Quick Trace

With QuickTrace, you can trace messages from specific loggers and store the messages in memory. Because QuickTrace logs the messages to memory, it avoids the cost of formatting, string manipulations, and input/output operations. As a result, you can enable fine-level application logging for specific loggers without performance overhead.

By default, QuickTrace writes the messages to one common buffer. However, you can specify that messages for particular users are written to separate buffers.

You can save the messages that are in memory to a file by invoking the QuickTrace Dump in Fusion Middleware Control as described in [Section 12.6.1.3.1](#) or by using the WLST, as described in [Section 12.6.1.3.2](#).

To enable QuickTrace, you create a QuickTrace handler and associate a logger with it. You can specify the buffer size, as well as other attributes, for the handler. Then, you set the level of the amount and type of information to be written by the loggers to memory.

12.6.1.2 Configuring QuickTrace

You can configure and use QuickTrace using Fusion Middleware Control or WLST, as described in the following topics:

- [Configuring QuickTrace Using Fusion Middleware Control](#)
- [Configuring QuickTrace Using WLST](#)

12.6.1.2.1 Configuring QuickTrace Using Fusion Middleware Control To configure QuickTrace using Fusion Middleware Control:

1. From the navigation pane, expand the domain. Right-click the Managed Server name and choose **Logs**, then **Log Configuration**.

The Log Configuration page is displayed.

2. Select the QuickTrace tab.
3. Click **Create**.

The Create QuickTrace Handler dialog box is displayed, as shown in the following figure:

4. For **Name**, enter a name for the handler.
5. For **Buffer Size**, enter the size, in bytes, for the buffer for storing log messages in memory. The default is 5242880.
6. For **Maximum Field Length**, enter the length, in bytes, for each field in a message. The fields can include the message text, supplemental attributes, and the thread name. The default is 240.

An excessively long field for each message can reduce the amount of log records in the buffer.

7. For **Handler Level**, select the log level for the handler. See [Section 12.4.3](#) for information about the levels.
8. For **Loggers to Associate**, select the loggers that you want to associate with this QuickTrace handler. All messages of the specified level for these handlers will be written to memory.

Many loggers are associated with other handlers. For example, the oracle.adf logger is associated with the handlers odl-handler, wls-domain, and console-handler. When you set the level of the logger, these handlers will use the same level, such as TRACE:1, for the logger, such as oracle.adf. As a result, much information will be written to the log files, consuming resources. To avoid

consuming resources, set the level of the handlers to a lower level, such as WARNING or INFORMATION.

9. Select **Enable User Buffer?** if you want to enable a user buffer. If you enable this, the handler maintains an individual buffer for each user you specify.

Then, for **User Names for Reserve Buffer**, enter the names of the users, separated by commas.

10. For the remaining options, accept the default values. For information about the options, see "ConfigureLogHandler" in the *WLST Command Reference for Infrastructure Components*.

11. Click **OK**.

12. When the configuration completes processing, click **OK**.

Now, messages of the specified level for the specified loggers are written to memory.

12.6.1.2.2 Configuring QuickTrace Using WLST To configure QuickTrace using WLST, you associate a logger with the QuickTrace handler, using the `configureLogHandler` command.

For example, to associate the `oracle.adf` logger with the QuickTrace handler and write all TRACE:1 messages to memory:

1. Use the `configureLogHandler` command to associate the logger with the QuickTrace handler:

```
configureLogHandler(name="quicktrace-handler", addToLogger="oracle.adf")
```

```
Handler Name: quicktrace-handler
type: oracle.core.ojdl.logging.QuickTraceHandlerFactory
encoding: UTF-8
maxFieldLength: 240
mode: objRef
useThreadName: false
useSourceClassandMethod: false
useLoggingContext: false
bufferSize: 5242880
```

The messages for the handler are written to a common buffer.

You can set additional properties for the QuickTrace handler. For example, to enable user buffers for the users `user1` and `user2`:

```
configureLogHandler(name="quicktrace-handler", addToLogger="oracle.adf.faces",
    propertyName="enableUserBuffer", propertyValue="true",
    propertyName="enableUserBuffer", propertyValue="user1, user2")
...
Handler Name: quicktrace-handler
type: oracle.core.ojdl.logging.QuickTraceHandlerFactory
useLoggingContext: false
bufferSize: 5242880
.
.
.
reserveBufferUserID: user1, user2
enableUserBuffer: true
```

Messages for `user1` and `user2` are written to separate buffers. In addition, messages related to other users are written to the common buffer.

To confirm the settings for the handler, use the `listLogHandlers` command, as described in "listLogHandlers" in the *WLST Command Reference for Infrastructure Components*.

2. Set the level of the logger, using the `setLogLevel` command:

```
setLogLevel(logger='oracle.adf', level='TRACE:1')
```

To confirm the settings for the logger, use the `listLoggers` command, as described in "listLoggers" in the *WLST Command Reference for Infrastructure Components*.

3. Many loggers are associated with other handlers. For example, the `oracle.adf` logger is associated with the handlers `odl-handler`, `wls-domain`, and `console-handler`. When you set the level of the logger, these handlers will use the same level (TRACE:1) for the logger `oracle.adf`. As a result, much information will be written to the log files, consuming resources. To avoid consuming resources, set the level of the handlers to a lower level, such as WARNING or INFORMATION.

For this example, set the level of the three handlers to WARNING:1:

```
configureLogHandler(name="odl-handler", level="WARNING:1")
configureLogHandler(name="wls-domain", level="WARNING:1")
configureLogHandler(name="console-handler", level="WARNING:1")
```

Note that you should keep the level of the QuickTrace handler at ALL, which is the default.

For more information, see "configureLogHandler" in the *WLST Command Reference for Infrastructure Components*

To confirm the level for the handler, use the `getLogLevel` command, as described in [Section 12.4.3.2](#).

12.6.1.3 Writing Trace Messages to a File

You can write trace messages to a file using Fusion Middleware Control or WLST, as described in the following topics:

- [Writing the Trace Messages to a File Using Fusion Middleware Control](#)
- [Writing the Trace Messages to a File Using WLST](#)

12.6.1.3.1 Writing the Trace Messages to a File Using Fusion Middleware Control You can save the messages that are in memory to a file by invoking the QuickTrace Dump in Fusion Middleware Control:

1. From the QuickTrace tab of the Log Configuration page, select the handler and click **Invoke QuickTrace Dump**.

The Invoke QuickTrace Dump dialog box is displayed.

2. For **Buffer Name**, if you have specified user buffers when you configured the QuickTrace handler, select the user, or select Common Buffer for users that you did not specify. If you did not specify any user buffers, the Common Buffer is the only option.
3. Click **OK**.

When the processing is complete, the View Log Messages page is displayed.

4. You can search the messages, as described in [Section 12.3.2](#), and you can correlate the messages as described in [Section 12.5](#).

In addition, you can download the messages to a file, as described in [Section 12.3.3.1](#).

12.6.1.3.2 Writing the Trace Messages to a File Using WLST You can save the messages to a file by using the `executeDump` command.

For example:

```
executeDump(name="odl.quicktrace", outputFile="/scratch/oracle1/qt1.dmp")
```

The command writes the dump to the specified file.

For more information about the `executeDump` command, see [Section 13.4.4.3](#).

In addition, if an incident is created (automatically or manually), the QuickTrace messages are written to dump files in the incident directory. If you enabled user buffers, each user will have one file and the common buffer will have one file.

The file names have the following format:

```
odl_quicktraceN_iincident_number.username.dmp
```

For example:

```
odl_quicktrace6_i1.weblogic.dmp
```

See [Section 13.4.6.1](#) for information about creating an incident.

12.6.1.4 Disabling QuickTrace Using WLST

To disable QuickTrace, use the WLST `configureLogHandler` command and specify that the level is OFF:

```
configureLogHandler(name="quicktrace-handler", level="OFF")
```

```
Handler Name: quicktrace-handler
type: oracle.core.ojdl.logging.QuicktraceHandlerFactory
.
.
.
reserveBufferUserID: user1, user2
enableUserBuffer: true
```

To remove a specific logger from association with the QuickTrace handler, use the `configureLogHandler` command with the `removeFromLogger` parameter:

```
configureLogHandler(name="quicktrace-handler",
removeFromLogger="oracle.adf.faces")
```

```
Handler Name: quicktrace-handler
type: oracle.core.ojdl.logging.QuicktraceHandlerFactory
reserveBufferUserID: user1, user2
enableUserBuffer: true
```

For more information, see "configureLogHandler" in the *WLST Command Reference for Infrastructure Components*.

12.6.2 Configuring and Using Selective Tracing

Selective tracing provides fine-grained logging for specified users or other attributes of a request.

The following topics describe selective tracing and how to manage it using Fusion Middleware Control or WLST:

- [Understanding Selective Tracing](#)
- [Configuring Selective Tracing](#)
- [Viewing Selective Traces](#)
- [Disabling Selective Tracing](#)

12.6.2.1 Understanding Selective Tracing

Selective tracing provides fine-grained logging for specified users or other attributes of a request.

For example, a user cannot perform some functions because of security permissions, but it is not clear what operations or lack of permission for those operations are posing a problem.

In this case, you can enable tracing across the entire system but this would generate a large volume of log messages for all users in the system, not only for the user having a problem. With selective tracing, you can enable tracing only for the user who is having a problem. Then, you can ask the user to retry the functions. Following that, you can look at the trace messages which apply to the specific request made by the user.

You can also specify the logger to narrow the scope of the messages being logged.

12.6.2.2 Configuring Selective Tracing


You can configure selective tracing using Fusion Middleware Control or WLST, as described in the following topics:



- [Configuring Selective Tracing Using Fusion Middleware Control](#)
- [Configuring Selective Tracing Using WLST](#)

12.6.2.2.1 Configuring Selective Tracing Using Fusion Middleware Control To configure selective tracing using Fusion Middleware Control:

1. From the navigation pane, right-click the domain name and choose **Logs**, then **Selective Tracing**.


The Selective Tracing page is displayed, as shown in the following figure:

soa_domain  Logged in as weblogic

 WebLogic Domain Page Refreshed Mar 20, 2014 6:58:38 AM PDT 

Selective Tracing

Use this page to configure the selective tracing settings.


 **Information**

Selective Tracing feature should be used only for critical diagnostics purposes. This feature adds more diagnostic logging messages and could be a performance impact. Enable Selective Tracing only for the needed tracing options.


Tracing Options Active Traces And Tracing History

Use this page for configuring selective tracing options. The configuration settings done on this page will be applied to all the Weblogic servers of the Weblogic domain.

Tracing Options

Application Name  Start Tracing


Add Fields


Level 


Description

Duration (minutes)

Trace ID Generate A New Unique Trace ID
 Use A Custom Trace ID

 **ODL**
 ODL logging events
 Enable

 **DMS**
 DMS data is composed of metrics that are created and updated by a broad range of Oracle components.
 Enable

 **Loggers**

2. For **Application Name**, select an application.
3. To add more fields, click **Add Fields** and select one of the options, such as Client Host or User Name.
4. For **Level**, select a logging level. [Table 12-3](#) describes the logging levels.
5. For **Description**, enter a description.
6. For **Duration**, enter the number of minutes that you want the selective trace to run.
 The selective trace is disabled after the specified time.
7. For Trace ID, select either **Generate a New Unique Trace ID** or **Use a Custom Trace ID**. If you select Use a Custom Trace ID, enter an ID of your choosing, but make sure that it is unique. Note Fusion Middleware Control does not verify the uniqueness of the ID.
8. In the ODL section, select **enable**.
9. In the DMS section, select **enable**.
10. In the Loggers section, by default, all loggers are selected.

You can select specific loggers that you want to trace. To find particular loggers, you can enter a string in the field above the table and click the Return key. For example, to find all loggers that begin with oracle.security, enter oracle.security.

Then, in the table, select the loggers in the **Enable on All Servers** column.

Note when you select loggers, those loggers apply to all current and active traces. Also note that even if you disable the loggers, you may see messages because all loggers have a general logging level, such as Notification. Those messages would still be written.

11. Click Start Tracing.

Now that you have started the trace, you can view active traces, as well as former traces, as described in [Section 12.6.2.3.1](#).

12.6.2.2.2 Configuring Selective Tracing Using WLST You can configure loggers for selective tracing and start tracing using the WLST `configureTracingLoggers` and `startTracing` commands.

For the simplest case, you can configure and start a trace using the `startTracing` command. When you do so, the selective tracing includes all loggers enabled for selective tracing.

For example, `user1` receives errors when attempting to perform certain operations. To start a trace of messages related to `user1` and to set the logging level to `FINE`, use the following command:

```
startTracing(user="user1", level="FINE")
Started tracing with ID: 885649f7-8efd-4a7a-9898-accbfc0bbba3
```

The `startTracing` command does not provide options to include or exclude particular loggers. In this case, you can use the `configureTracingLoggers` command. This command allows you to configure selective tracing to include only particular loggers and particular Oracle WebLogic Server instances. Note that the options you specify apply to all current and active traces.

For example, to configure selective tracing to include only security-related loggers:

1. Specify that all loggers be disabled for tracing, as shown in the following example:

```
configureTracingLoggers(action="disable")
Configured 1244 loggers
```

2. Enable the security-related loggers, by specifying the `pattern` option with a regular expression:

```
configureTracingLoggers(pattern='oracle.security.*', action="enable")
Configured 62 loggers
```

To see a list of the loggers that support selective tracing, use the WLST `listTracingLoggers` command, as shown in the following example:

```
listTracingLoggers(pattern="oracle.security.*")
-----+-----
Logger                                     | Status
-----+-----
oracle.security                           | enabled
oracle.security.audit.logger               | enabled
oracle.security.jps.az.common.util.JpsLock | enabled
.
.
.
```

3. Use the `startTracing` command, specifying the users and the level. For example:

```
startTracing(user="user1", level="FINE")
Started tracing with ID: a9580e65-13c4-420b-977e-5ba7dd88ca7f
```


See Also: The following commands in the *WLST Command Reference for Infrastructure Components* for complete syntax:

- "configureTracingLoggers"
- "startTracing"
- "listTracingLoggers"

12.6.2.3 Viewing Selective Traces

You can view selective traces using Fusion Middleware Control or WLST, as described in the following topics:

- [Viewing Selective Traces Using Fusion Middleware Control](#)
- [Viewing Selective Traces Using WLST](#)

12.6.2.3.1 Viewing Selective Traces Using Fusion Middleware Control You can view the selective traces that are currently active and the history of selective traces.

To view the selective traces:

1. From the Selective Tracing page, select the **Active Traces and Tracing History** tab.

The tab shows a table with the active traces and a table with the tracing history, as shown in the following figure:

The screenshot shows the 'Selective Tracing' page with the 'Active Traces And Tracing History' tab selected. The page includes an information section and two tables. The 'Active Traces' table has the following data:

Trace ID	Option Name	Option Value	Description	Start
5c461fb3-88c7-4865-9c11-606cf41afb6	Application Name	testapp1a		Mar 2

The 'Tracing History' table is empty, with the text 'No tracing history' displayed below it.

2. To view a trace, select it from the appropriate table.

The Log Messages page is displayed, with the messages that were captured by Selective Tracing. You can search the messages, as described in [Section 12.3.2](#), and you can correlate the messages as described in [Section 12.5](#).

In addition, you can download the messages to a file, as described in [Section 12.3.3.1](#).

12.6.2.3.2 Viewing Selective Traces Using WLST After you have begun a trace, you can see the active traces by using the `listActiveTraces` command, as shown in the following example:

```
listActiveTraces()
-----+-----+-----+-----+-----+-----
Trace ID                               |Attr. Name|Attr. Value| Level| Exp. Time |Description
-----+-----+-----+-----+-----+-----
b73b351c-9a9b-47df-b05a-356a336d5780 | USER_ID | user1     | FINE | 5/22/13 11:17 AM |
a9580e65-13c4-420b-977e-5ba7dd88ca7f | USER_ID | user1     | FINE | 5/22/13 11:19 AM |
```

You can view the contents of the trace using the `displayLogs` command and passing it the trace ID. You can also view traces that have stopped. For example:

```
displayLogs("a9580e65-13c4-420b-977e-5ba7dd88ca7f")
```

See "listActiveTraces" in the *WLST Command Reference for Infrastructure Components* for complete syntax.

12.6.2.4 Disabling Selective Tracing

You can configure selective tracing, view traces, and disable selective tracing using WLST, as described in the following topics:

- [Disabling Selective Tracing Using Fusion Middleware Control](#)
- [Disabling Selective Traces Using WLST](#)

12.6.2.4.1 Disabling Selective Tracing Using Fusion Middleware Control To disable selective tracing using Fusion Middleware Control:

1. From the navigation pane, right-click the domain name and choose **Logs**, then **Selective Tracing**.
2. Select the **Active Traces and Tracing History** tab.
3. In the Active Traces table, select the trace and click **Disable**.

12.6.2.4.2 Disabling Selective Traces Using WLST To avoid excessive logging in the system, you can disable a selective trace when you have obtained the information that you need. To disable a selective trace, you use the WLST `stopTracing` command, passing it the trace ID or user. For example:

```
stopTracing(traceId="885649f7-8efd-4a7a-9898-accbfc0bbba3")
Stopped 1 traces
```

You can also disable all traces by using the `stopAll` option. For example:

```
stopTracing(stopAll=1)
```

See "stopTracing" in the *WLST Command Reference for Infrastructure Components* for complete syntax

Diagnosing Problems

This chapter describes how to use the Oracle Fusion Middleware Diagnostic Framework to collect and manage information about a problem so that you can resolve it or send it to Oracle Support for resolution.

This chapter contains the following sections:

- [Section 13.1, "Understanding the Diagnostic Framework"](#)
- [Section 13.2, "How the Diagnostic Framework Works"](#)
- [Section 13.3, "Configuring the Diagnostic Framework"](#)
- [Section 13.4, "Investigating, Reporting, and Solving a Problem"](#)
- [Section 13.5, "Managing and Running the Health Test Framework"](#)

13.1 Understanding the Diagnostic Framework

Oracle Fusion Middleware includes a Diagnostic Framework, which aids in detecting, diagnosing, and resolving problems. The problems that are targeted in particular are critical errors, such as those caused by code bugs, metadata corruption, customer data corruption, deadlocked threads, and inconsistent state.

When a critical error occurs, it is assigned an incident number, and diagnostic data for the error (such as log files) are immediately captured and tagged with this number. The data is then stored in the Automatic Diagnostic Repository (ADR), where it can later be retrieved by incident number and analyzed.

The goals of the Diagnostic Framework are:

- First-failure diagnosis
- Limiting damage and interruptions after a problem is detected
- Reducing problem diagnostic time
- Reducing problem resolution time
- Simplifying customer interaction with Oracle Support

The Diagnostic Framework includes the following technologies:

- **Automatic capture of diagnostic data upon first failure:** For critical errors, the ability to capture error information at first failure greatly increases the chance of a quick problem resolution and reduced downtime. The Diagnostic Framework automatically collects diagnostics, such as thread dumps, DMS metric dumps, and WebLogic Diagnostics Framework (WLDF) server image dumps. Such diagnostic data is similar to the data collected by airplane "black box" flight recorders. When a problem is detected, alerts are generated and the fault diagnosability

infrastructure is activated to capture and store diagnostic data. The data is stored in a file-based repository and is accessible with command-line utilities.

- **Standardized log formats:** Standardized log formats (using the ODL log file format) across all Oracle Fusion Middleware components allows administrators and Oracle Support personnel to use a single set of tools for problem analysis. Problems are more easily diagnosed, and downtime is reduced.
- **Diagnostic rules:** Each component defines diagnostic rules that are used to evaluate whether a given log message should result in an incident being created and which dumps should be executed. The diagnostic rules also indicate whether an individual dump should be created synchronously or asynchronously.

In addition, you can define custom rules that apply to a domain, a server, or an application in a domain or server.

- **Incident detection log filter:** The incident detection log filter implements the `java.util.logging` filter. It inspects each log message to see if an incident should be created, basing its decision on the diagnostic rules for components and applications.
- **Incident packaging service (IPS) and incident packages:** The IPS enables you to automatically and easily gather the diagnostic data—log files, dumps, reports, and more—pertaining to a critical error that has a corresponding incident, and package the data into a zip file for transmission to Oracle Support. All diagnostic data relating to a critical error that has been detected by the Diagnostics Framework is captured and stored as an incident in ADR. The incident packaging service identifies the required files automatically and adds them to the zip file.

Before creating the zip file, the IPS first collects diagnostic data into an intermediate logical structure called an incident **package**. Packages are stored in the Automatic Diagnostic Repository. If you choose to, you can access this intermediate logical structure, view and modify its contents, add or remove additional diagnostic data at any time, and when you are ready, create the zip file from the package and upload it to Oracle Support.

- **Integration with WebLogic Diagnostics Framework (WLDF):** The Oracle Fusion Middleware Diagnostics Framework integrates with some features of WebLogic Diagnostics Framework (WLDF), including the capturing of WebLogic Server images on detection of critical errors. WLDF is a monitoring and diagnostic framework that defines and implements a set of services that run within WebLogic Server processes and participate in the standard server life cycle. Using WLDF, you can create, collect, analyze, archive, and access diagnostic data generated by a running server and the applications deployed within its containers. This data provides insight into the run-time performance of servers and applications and enables you to isolate and diagnose faults when they occur.

Oracle Fusion Middleware Diagnostics Framework integrates with the following components of WLDF:

- WLDF Watch and Notification, which watches specific logs and metrics for specified conditions and sends a notification when a condition is met. There are several types of notifications, including JMX notification and a notification to create a Diagnostic Image. Oracle Fusion Middleware Diagnostics Framework integrates with the WLDF Watch and Notification component to create incidents.
- Diagnostic Image Capture, which gathers the most common sources of the key server state used in diagnosing problems. It packages that state into a single

artifact, the Diagnostic Image. With Oracle Fusion Middleware Diagnostics Framework, it writes the artifact to ADR.

For more information about WLDF, see *Configuring and Using the Diagnostics Framework for Oracle WebLogic Server*.

13.1.1 About Incidents and Problems

To facilitate diagnosis and resolution of critical errors, the Diagnostic Framework introduces two concepts for Oracle Fusion Middleware: problems and incidents.

A **problem** is a critical error. Critical errors manifest as internal errors or other severe errors. Problems are tracked in the ADR. Each problem has a **problem key**, which is a text string that describes the problem. It includes an error code (in the format *XXX-nnnnn*) and in some cases, other error-specific values.

An **incident** is a single occurrence of a problem. When a problem (critical error) occurs multiple times, an incident is created for each occurrence. Incidents are timestamped and tracked in the ADR. Each incident is identified by a numeric incident ID, which is unique within the ADR home. When an incident occurs, the Diagnostic Framework:

- Gathers first-failure diagnostic data about the incident in the form of dump files (incident dumps).
- Stores the incident dumps in an ADR subdirectory created for that incident.
- Registers the incidents dumps with the incident in ADR.

13.1.1.1 Incident Flood Control

It is conceivable that a problem could generate dozens or perhaps hundreds of incidents in a short period of time. This would generate too much diagnostic data, which would consume too much space in the ADR and could possibly slow down your efforts to diagnose and resolve the problem. For these reasons, the Diagnostic Framework applies flood control to incident generation after certain thresholds are reached. A **flood-controlled incident** is an incident that is not recorded in the ADR. Instead, the Diagnostic Framework writes a message at the WARNING level to the log file and returns an `oracle.dfw.incident.Incident` object. Flood-controlled incidents provide a way of informing you that a critical error is ongoing, without overloading the system with diagnostic data.

By default, if more than 5 incidents with the same problem key occur within 60 minutes, subsequent incidents with the same problem key are flood controlled. You can change this value using MBeans, as described in [Section 13.3](#).

13.1.2 Diagnostic Framework Components

The following topics describe the key components of the Diagnostic Framework:

- [Automatic Diagnostic Repository](#)
- [Diagnostic Dumps](#)
- [Management MBeans](#)
- [WLST Commands for Diagnostic Framework](#)
- [ADRCI Command-Line Utility](#)

Note: To use the Diagnostic Framework, in particular the Automatic Diagnostic Repository, the Managed Servers must have Oracle JRF applied. The following directory will exist for each Managed Server if Oracle JRF has been applied:

DOMAIN_HOME/SERVERS/server_name/adr

If the directory does not exist take one of the following steps:

- Apply Oracle JRF, as described in [Section 19.3.1](#).
 - If Oracle JRF has been applied, restart the servers, making sure that the Node Manager property `startScriptEnabled` is set to `true`, as described in [Section 2.7.1](#).
-
-

13.1.2.1 Automatic Diagnostic Repository

The Automatic Diagnostic Repository (ADR) is a file-based hierarchical repository for Oracle Fusion Middleware diagnostic data, such as traces and dumps. The Oracle Fusion Middleware components store all incident data in the ADR. Each Oracle WebLogic Server stores diagnostic data in subdirectories of its own home directory within the ADR. For example, each Managed Server and Administration Server has an ADR home directory.

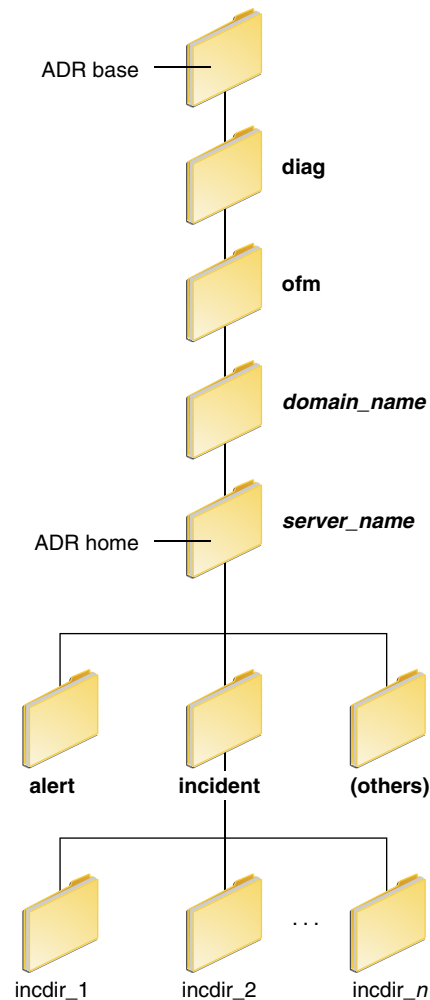
The ADR root directory is known as ADR base. By default, the ADR base is located in the following directory:

DOMAIN_HOME/servers/server_name/adr

Within ADR base, there can be multiple ADR homes, where each ADR home is the root directory for all incident data for a particular instance of Oracle WebLogic Server. The following path shows the location of the ADR home:

ADR_BASE/diag/ofm/domain_name/server_name

[Figure 13–1](#) illustrates the directory hierarchy of the ADR home for an Oracle WebLogic Server instance.

Figure 13–1 ADR Directory Structure for Oracle Fusion Middleware

The subdirectories in the ADR home contain the following information:

- alert: The XML-formatted alert log.
- incident: A directory that can contain multiple subdirectories, where each subdirectory is named for a particular incident. The subdirectories are named `incdir_n`, with *n* representing the number of the incident. Each subdirectory contains information and diagnostic dumps pertaining only to that incident.
- (others): Other subdirectories of ADR home, which store incident packages and other information.

Note: ADR uses the domain name as the Product ID and the server name as the Instance ID when it packages an incident. However, if either name is more than 30 characters, ADR truncates the name. In addition, dollar sign (\$) and space characters are replaced with underscores.

13.1.2.2 Diagnostic Dumps

A **diagnostic dump** captures and dumps specific diagnostic information when an incident is created (automatic) or on the request of an administrator (manual). When executed as part of incident creation, the dump is included with the set of incident diagnostics data. Examples of diagnostic dumps include a JVM thread dump, JVM class histogram dump, and DMS metric dump. For a list of diagnostic dumps, see [Table 13-7](#).

13.1.2.3 Management MBeans

The Diagnostic Framework provides MBeans that you can use to configure the Diagnostic Framework. For example, you can enable or disable flood control and you can configure how many incidents with the same problem key can occur within a specified time period. For information about using the management MBeans to configure the Diagnostic Framework, see [Section 13.3](#).

You can also use the MBeans to query and create incidents, discover the list of available diagnostic dump types, and execute individual diagnostic dumps.

13.1.2.4 WLST Commands for Diagnostic Framework

The Diagnostic Framework provides WLST commands that you can use to view information about problems and incidents, create incidents, execute specific dumps and query the set of diagnostic dump types. For more information, see:

- [Viewing Problems](#)
- [Viewing Incidents](#)
- [Listing Diagnostic Dumps](#)
- [Viewing a Description of a Diagnostic Dump](#)
- [Executing Dumps](#)
- [Creating an Incident Manually](#)
- "Diagnostic Framework Custom WLST Commands" in the *WLST Command Reference for Infrastructure Components*

To use the custom WLST Diagnostic Framework commands, you must invoke the WLST script from the Oracle Common home. See [Section 2.4.2](#) for more information.

13.1.2.5 ADRCI Command-Line Utility

The ADR Command Interpreter (ADRCI) is a utility that enables you to investigate problems, and package and upload first-failure diagnostic data to Oracle Support, all within a command-line environment. ADRCI also enables you to view the names of the dump files in the ADR, and to view the alert log with XML tags stripped, with and without content filtering.

ADRCI is installed in the following directory:

```
(UNIX) ORACLE_HOME/oracle_common/adr  
(Windows) ORACLE_HOME\oracle_common\adr
```

See the following sections for information about using the ADRCI command-line utility:

- [Section 13.4.6.3](#) for information on packaging an incident.
- [Section 13.4.6.4](#) for information on purging incidents.

See Also:

- The chapter "ADRCI: ADR Command Interpreter" in *Oracle Database Utilities*
- The chapter "Managing Diagnostic Data" in the *Oracle Database Administrator's Guide*

13.2 How the Diagnostic Framework Works

The Diagnostic Framework is active in each server and provides automatic error detection through predefined configured rules. Oracle Fusion Middleware components and applications automatically benefit from this always-on checking.

Incidents are automatically detected in two ways:

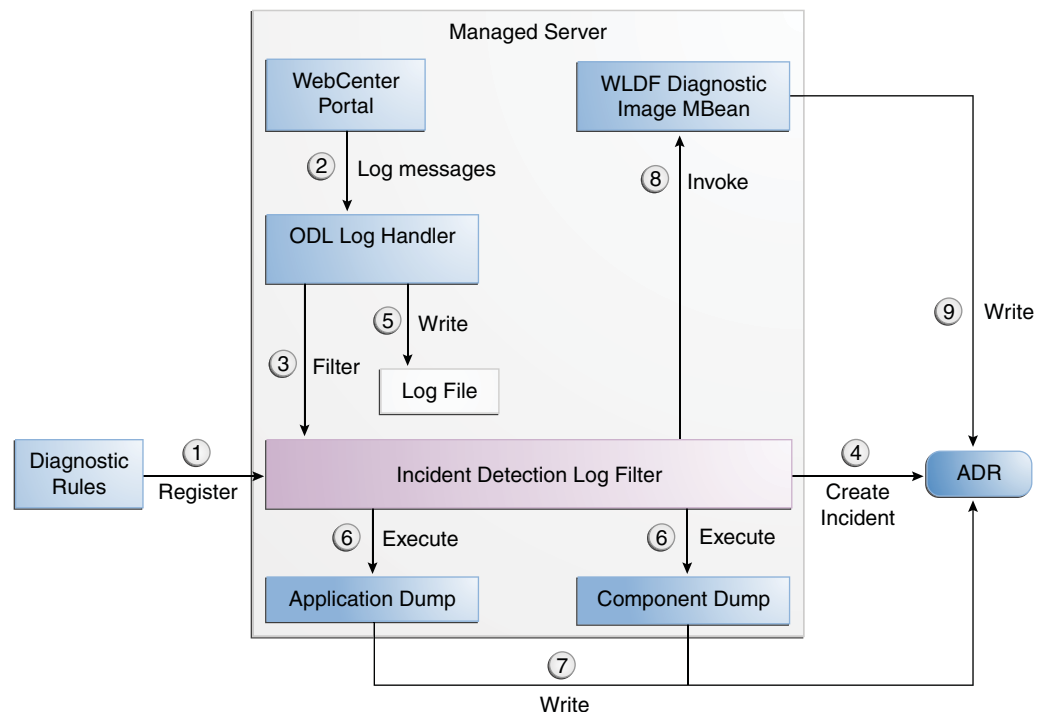
- By the incident detection log filter, which is automatically configured to detect critical errors.
- By the WLDF Watch and Notification component. The Diagnostics Framework listens for a predefined notification type and creates incidents when it receives such notifications.

For information about configuring WLDF Watch and Notification, see [Section 13.3.4](#).

- Programmatic incident creation. Some components create incidents directly.

[Figure 13–2](#) shows the interaction when the incident is detected by the incident log detector. It shows the interaction among the incident log detector, the WLDF Diagnostic Image MBean, ADR, and component or application dumps when an incident is detected by the incident log detector.

Figure 13–2 Incident Creation Generated by Incident Log Detector



The steps represented in [Figure 13–2](#) are:

1. The incident detection log filter is initialized with component and application diagnostic rules.
2. An application or component logs a message using the java.util.logging API.
3. The ODL log handler passes the message to the incident detection log filter.
4. The incident log detection filter inspects the log message to see if an incident should be created, basing its decision on the diagnostic rules for the component. If the diagnostic rule indicates that an incident should be created, it creates an incident in the ADR.
5. The ODL log handler writes the log message to the log file, and returns control to the application.

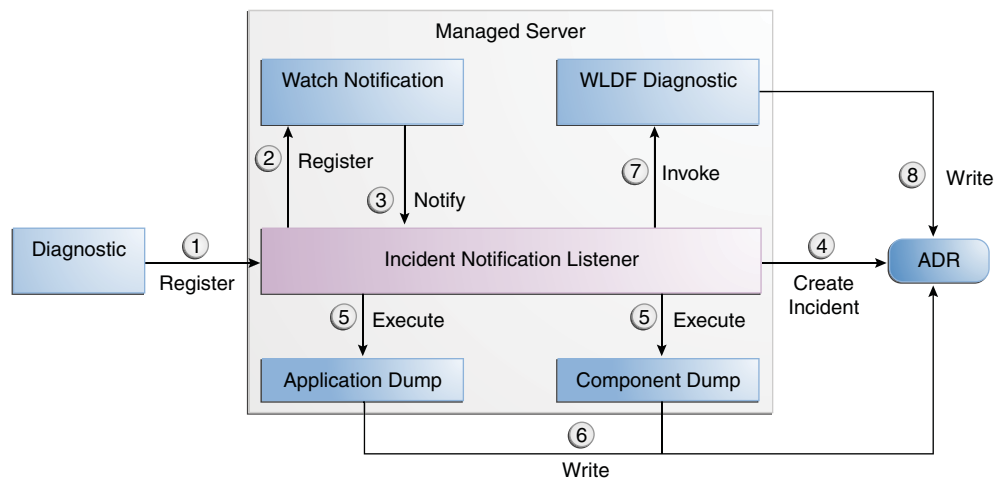
When an incident is created, a message, similar to the following, is written to the log file:

```
[2014-03-28T11:05:34.603-07:00] [wls_server_1] [NOTIFICATION] [DFW-40101]
[oracle.dfw.incident] [tid: [ACTIVE].ExecuteThread: '4' for queue:
'weblogic.kernel.Default (self-tuning)'] [userId: weblogic] [ecid:
66217af9-247f-4344-94a9-14f90e75a586-000e093f,0] An incident has been signalled
with the incident facts: [problemKey=MDS-50500 [MANUAL] incidentSource=MANUAL
incidentTime=Fri March 28 11:05:34 PDT 2014 errorMessage=MDS-50500
executionContextId=null]
```

6. The Diagnostic Framework executes the diagnostic dumps that are indicated by the diagnostic rules for the component.
7. The Diagnostic Framework writes the dumps to ADR, in the directory created for the incident.
8. The Diagnostic Framework invokes the WLDF Diagnostic Image MBean requesting that a Diagnostic Image be created in ADR.
9. WLDF writes the Diagnostic Image to ADR.

Figure 13–3 shows the interaction when an incident is detected by the WLDF Watch and Notification system. It shows the interaction among the incident notification listener, the WLDF Watch and Notification system, and the WLDF Diagnostic Image MBean.

Figure 13–3 Incident Creation Generated by WLDF Watch Notification



The steps represented in [Figure 13–3](#) are:

1. The incident notification listener is initialized with component and application diagnostic rules.
2. Oracle Fusion Middleware Diagnostic Framework registers a JMX notification listener with WLDF. The listener listens for events from the WLDF Watch and Notification system. It only processes notifications of type `oracle.dfw.wldfnotification`.
3. Something in the system causes the configured WLDF watch to be triggered, causing a notification to be sent to the incident notification listener. The notification includes event information describing the data that caused the watch to trigger.
4. The Diagnostic Framework creates an incident in ADR.
5. The Diagnostic Framework executes the diagnostic dumps that are indicated by the diagnostic rules.
6. The Diagnostic Framework writes the dumps to ADR, in the directory created for the incident.
7. The Diagnostic Framework invokes the WLDF Diagnostic Image MBean requesting that a Diagnostic Image be created in ADR.
8. WLDF writes the Diagnostic Image to ADR.

13.3 Configuring the Diagnostic Framework

You can configure some settings for the Diagnostic Framework. In addition, you can configure an WLDF Watch and Notification to create an incident. The following topics describe how to configure the Diagnostic Framework:

- [Configuring Diagnostic Framework Settings](#)
- [Configuring Custom Diagnostic Rules](#)
- [Configuring Problem Suppression](#)
- [Configuring WLDF Watch and Notification for the Diagnostic Framework](#)

13.3.1 Configuring Diagnostic Framework Settings

You can configure the following settings:

- Enabling or disabling the detection of incidents through the log files
- Enabling or disabling flood control and setting parameters for flood control

You configure these settings by using the Diagnostic Framework MBean `DiagnosticConfig`. The following shows the MBean's `ObjectName`:

```
oracle.dfw:type=oracle.dfw.jmx.DiagnosticsConfigMBean,name=DiagnosticsConfig
```

[Table 13–1](#) shows the attributes for the `DiagnosticConfig` MBean and a description of each parameter.

Table 13–1 DiagnosticConfig MBean Attributes for Diagnostic Framework

Attributes	Description
DumpSamplingIdleWhenHealthy	Determines whether dump sampling is active when the system is healthy. By default, this is set to <code>true</code> , which means that dump sampling is not active until an incident occurs.
DumpSamplingMinimumHealthyPeriod	The amount of time in seconds that the dump sampling is active after an incident occurs. The default is 259200 seconds (72 hours).
floodControlEnabled	Enables or disables flood control. Specify <code>true</code> for enabled or <code>false</code> for disabled. The default is <code>true</code> . Note that flood control does not apply to manually created incidents.
floodControlIncidentCount	Sets the number of incidents with the same problem key that can be created within the time period, specified by <code>floodControlIncidentTimeoutPeriod</code> , before they are controlled by flood control. The default is 5. When flood control is enabled, if the number of incidents with the same problem key exceeds this count, no incidents are created, but the Diagnostic Framework writes a message at the <code>WARNING</code> level to the log file.
floodControlIncidentTimeoutPeriod	Sets the time period in which the number of incidents, as specified by <code>floodControlIncidentCount</code> , with the same problem key can be created before they are controlled by flood control. The default is 60 minutes.
incidentCreationEnabled	Enables or disables incident creation. Specify <code>true</code> for enabled or <code>false</code> for disabled. The default is <code>true</code> .
logDetectionEnabled	Enables or disables the detection of incidents through the log files. Specify <code>true</code> for enabled or <code>false</code> for disabled. The default is <code>true</code> .
maxTotalIncidentSize	Sets the maximum total size that is allocated for all incidents. When the limit is reached, the oldest incidents are purged until the space used by all incidents is less than the amount specified by this parameter. The default is 500 MB. The limit may be exceeded during the creation of an incident, but when the incident creation completes, the oldest incidents are purged.
reservedMemoryKB	The amount of reserved memory that is released when <code>OutOfMemoryError</code> is detected. When the Diagnostic Framework starts, it allocates 512 KB of memory for its own private use. When the Diagnostic Framework detects that an <code>OutOfMemoryError</code> has occurred in the server, it frees that block of memory and proceeds to create the incident. The default is 512 KB.
uncaughtExceptionDetectionEnabled	Enables the Java-based uncaught exception handler. When enabled and an uncaught exception is detected, an incident is created. Specify <code>true</code> for enabled or <code>false</code> for disabled. The default is <code>true</code> .

Table 13–1 (Cont.) DiagnosticConfig MBean Attributes for Diagnostic Framework

Attributes	Description
useExternalCommands	Indicates whether external JVM commands should be used to perform thread dumps. Specify <code>true</code> for enabled or <code>false</code> for disabled. The default is <code>true</code> .

The following example shows how to configure these settings using the Fusion Middleware Control System MBean Browser:

1. From the WebLogic Domain menu, choose **System MBean Browser**.
The System MBean Browser page is displayed.
2. Expand **Application Defined Beans**, then **oracle.dfw**, then **domain.domain_name**, then **dfw.jmx.DiagnosticsConfigMBean**.
3. Select one of the **DiagnosticConfig** entries. There is one DiagnosticConfig entry for each server.
4. In the Application Defined MBean pane, expand **Show MBean Information** to see the server name.

The following shows the System MBean Browser page:

The screenshot shows the System MBean Browser interface for the domain 'soa_domain'. The left pane shows a tree view of the domain structure, with 'oracle.dfw.jmx.DiagnosticsConfig' selected. The right pane shows the 'Application Defined MBeans: oracle.dfw.jn...' configuration page. The 'Information' section indicates that changes are not managed by the configuration session. The 'Hide MBean Information' section shows the MBean Name and Description. The 'Attributes' section is expanded, showing a table of attributes:

Name	Description
1 ConfigMBean	If true, it indicates that this MBean
2 DumpSamplingEnabled	Diagnostic Dump Sampling enabled
3 DumpSamplingIdleWhenHealthy	Dump Sampling is idle or not based
4 DumpSamplingMinimumHealthyPeriod	The minimum period that is used f
5 eventProvider	If true, it indicates that this MBean
6 eventTypes	All the event's types emitted by t
7 FloodControlEnabled	Incident flood control enabled/dis
8 FloodControlIncidentCount	The number of incidents that can
9 FloodControlIncidentTimePeriod	The time span of flood control in r

5. To change the values for the attributes listed in Table 13–1, enter or select the value in the **Value** field.
6. Click **Apply**.

13.3.2 Configuring Custom Diagnostic Rules

You can configure custom diagnostic rules that apply to a domain, a server, or an application in a domain or server.

You create the custom diagnostic rules by creating an .xml file with a particular format, which is shown in the example later in this section. You must save the file to one of the following locations:

- For rules that apply to the entire domain:

`DOMAIN_HOME/config/fmwconfig/dfw`

- For rules that apply to a particular server:

`DOMAIN_HOME/config/fmwconfig/servers/server_name/dfw`

The file name must use the following format:

`name.xml`
`appname#name.xml`

In the format, *appname* is the name of the application to which the rule applies. The *appname* must be the exact name of the deployed application. *name* is the name of the rule you specify. If you do not specify *appname*, the rules will apply to the entire server. For example, the following rule applies to the application myApp:

`myApp#custom_rule.xml`

The custom diagnostic rules file can contain the following types of elements to define the rule:

- Log detection conditions, which are optional

You can define a set of conditions, in the `logDetectionConditions` element, to check for in the diagnostic logs applicable to the server or to the specified application against which that the rules are registered. When a log message matching the condition is detected, an incident is created, capturing diagnostics that will help identify the problem. By default, all `INCIDENT_ERROR` messages are detected and an incident created for them. In addition, specific components may have configured rules to detect specific messages.

The following example shows a fragment of a custom diagnostic rules file that defines four log detection conditions. If one or more of the conditions are true, an incident is created.

```
<?xml version="1.0" encoding="UTF-8"?>
<diagnosticRules xmlns="http://www.oracle.com/DFW/DiagnosticsFrameworkRules"
xmlns:xs="http://www.w3.org/2001/XMLSchema-instance">
  <logDetectionConditions>
    <condition messageSeverity="INCIDENT_ERROR"/>
    <condition messageSeverity="ERROR" component="jrfServer_admin"/>
    <condition messageSeverity="ERROR" module="test.servletA"/>
    <condition messageId="FMW-40300"/>
  </logDetectionConditions>
```

See [Table 13–2](#) for a description of the conditions you can use.

- Processing rules

You can define processing rules that are evaluated when either the server or application rules are involved in incident creation. For example, if the application MyApp is involved in incident creation, any rules associated with the MyApp

application are evaluated. In all cases, server-wide rules are evaluated regardless of the application.

Processing rules consist of two parts:

- Default actions, which are optional. If they are present, they are always executed during incident creation. The actions are a list of diagnostic dumps to execute, along with optional arguments.

The following shows an example set of default actions:

```
<defaultActions>
  <dumpAction name="odl.logs">
    <argument name="timestamp" value="INCIDENT_TIME" valueType="fact"/>
  </dumpAction>
  <dumpAction name="dms.metrics"/>
</defaultActions>
```

See [Table 13–3](#) for a description of the optional arguments that you can use.

- Condition-based actions, which are executed only if the condition evaluates to true. Each `<rule>` element consists of a name attribute, along with a child `<ruleCondition>` element and a child `<ruleActions>` element. The `<ruleActions>` element contains one or more `dumpAction` elements. See [Table 13–4](#) for a list of the `<ruleCondition>` element attributes.

If multiple `<condition>` elements are specified in a single `<rule>` element, the `dumpAction` is executed only if all conditions evaluate to true.

The following shows an example of a condition-based action rule. If the `MESSAGE_ID` is `DFW-99997`, the condition evaluates to true and the `jvm.classhistogram` dump is executed.

```
<processingRules>
  <rule name="OOME">
    <ruleCondition>
      <condition name="MESSAGE_ID" value="DFW-99997"/>
    </ruleCondition>
    <ruleActions>
      <dumpAction name="jvm.classhistogram"/>
    </ruleActions>
  </rule>
</processingRules>
```

[Table 13–2](#) describes the attributes you can use to create the log detection conditions:

Table 13–2 Conditions for the `LogDetectionConditions` Element

Condition	Description
messageSeverity	The log level at which the message was logged. (This is the <code>MESSAGE_LEVEL</code> field for ODL log files.) For example, <code>INCIDENT_ERROR</code> , <code>ERROR</code> .
messageId	The ID of the message. (This is the <code>MESSAGE_ID</code> field for ODL log files.) For example, <code>DFW-99997</code> .
component	The component name. (This is the <code>COMPONENT_ID</code> field for ODL log files.) For example, <code>oracle.mds</code> .
module	The name of the module that originated the message. (This is the <code>MODULE_ID</code> field for ODL log files.)

See [Table 12–1](#) for a description of the ODL log file fields.

Table 13–3 describes the optional arguments that you can use for the <defaultActions> element.

Table 13–3 Optional arguments for the defaultActions Element

Argument	Description
name	The name of the argument.
value	The value of the argument
type	The type of argument. Valid values are: <ul style="list-style-type: none"> ▪ <code>literal</code>: If you specify this type, the literal value of the argument is used. This is the default. ▪ <code>fact</code>: If you specify this type, the value must be either <code>INCIDENT_TIME</code> or <code>ECID</code>. ▪ <code>context</code>: If you specify this type, the value must be the name of a value in the DMS Execution Context. For information on the DMS Execution Context, see "DMS Execution Context" in <i>Tuning Performance</i>.

Table 13–4 shows the <ruleCondition> element attributes.

Table 13–4 Attributes for the ruleCondition Element

Element	Description
name	The name of the attribute. Valid values depend on the valueType: <ul style="list-style-type: none"> ▪ If the valueType is <code>fact</code>, valid values are <code>COMPONENT_ID</code>, <code>MODULE_ID</code>, or <code>MESSAGE_ID</code>. ▪ If the valueType is <code>context</code>, the value must be the name of a value in the DMS Execution Context. For information on the DMS Execution Context, see "DMS Execution Context" in <i>Tuning Performance</i>.
operator	The operator. Value values are <code>EQ</code> , <code>EQNoCase</code> , <code>NE</code> , <code>Contains</code> , <code>StartsWith</code> , <code>EndsWith</code> , <code>LT</code> , <code>GT</code> , <code>LE</code> , <code>GE</code> . The default is <code>EQ</code> . The values are case sensitive.
value	The literal value to compare.
datatype	The data type. Valid values are <code>String</code> or <code>Integer</code> . The default is <code>String</code> . The values are case sensitive.
valueType	The type of argument: <ul style="list-style-type: none"> ▪ <code>fact</code> ▪ <code>context</code>

To create and load a custom diagnostic rule:

1. Create a file that contains the custom rules.

The following shows a sample custom rules file:

```
<?xml version="1.0" encoding="UTF-8"?>
<diagnosticRules xmlns="http://www.oracle.com/DFW/DiagnosticsFrameworkRules"
xmlns:xs="http://www.w3.org/2001/XMLSchema-instance">

  <logDetectionConditions>
```



```

<condition messageSeverity="INCIDENT_ERROR"/>
    // detect all message logged at level INCIDENT_ERROR
<condition messageSeverity="ERROR" component="jrfServer_admin"/>
    // detect all "jrfServer_admin" component messages logged at level
ERROR
<condition messageSeverity="ERROR" module="test.servletA"/>
    // detect all "test.servlet" module messages logged at level ERROR
<condition messageId="FMW-40300"/>
    // detect message "FMW-40300"
</logDetectionConditions>

<defaultActions>
<dumpAction name="odl.logs">
    <argument name="timestamp" value="INCIDENT_TIME" valueType="fact"/>
</dumpAction>
<dumpAction name="dms.metrics"/>
</defaultActions>

<processingRules>
<rule name="OOME">
<ruleCondition>
    <condition name="MESSAGE_ID" value="DFW-99997"/>
</ruleCondition>
<ruleActions>
    <dumpAction name="jvm.classshistogram"/>
</ruleActions>
</rule>
</processingRules>

</diagnosticRules>

```

2. Save the file, naming it with the extension `.xml`. If the rule applies to an application, precede the file name with `app_name#`. Save the file to one of the following locations:

```

DOMAIN_HOME/config/fmwconfig/dfw
DOMAIN_HOME/config/fmwconfig/servers/server_name/dfw

```

3. Load the rules, using the WLST command `reloadCustomRules`. The following example loads the rule `customrules.xml`, which applies to the application `myApp`:

```

reloadCustomRules (name='myApp#customrules.xml')

```

You can reload all the rules in the domain or all the rules that pertain to a particular server. The following example reloads all the rules for the server `wls_server1`:

```

reloadCustomRules (server='wls_server1')

```

For more information about the `reloadCustomRules` command, see "reloadCustomRules" in the *WLST Command Reference for Infrastructure Components*.

13.3.3 Configuring Problem Suppression

In certain situations, you may want to suppress the creation of incidents based on a particular problem key. For example, in a development environment, when you are developing a servlet, you may generate high number of uncaught exceptions as you refine the code. This results in the creation of unnecessary incidents.

The Diagnostic Framework allows you to configure problem suppression filters so that problems that match the filter criteria do not result in the creation of an incident.

When you configure a problem suppression filter, you use a regular expression that represents a pattern that you want to match. The regular expression is matched using the `java.util.regex` class. For example:

- The following regular expression matches any incident with a problem key that starts with MDS-5000.
`MDS-5000.*`
- The following regular expression matches any problem with the text `OutOfMemory`. Because the regular expression is case-sensitive, it will not match problems with the text `outofmemory`.
`.*OutOfMemory.*`

You can add and remove filters and get a list of filters or the detail of one filter using the `DiagnosticConfig` MBean.

Table 13–5 shows the operations and attribute for configuring problem suppression filters and a description of each.

Table 13–5 DiagnosticConfig MBean Operations and Attributes for Problem Suppression Filters

Operations and Attribute	Description
Operation: <code>addProblemKeyFilter(filter_pattern)</code>	Adds a new problem suppression filter. You pass it the regular expression that represents a pattern that you want to match. For example: <code>addProblemKeyFilter(".*OutOfMemory.*")</code>
Attribute: <code>getProblemKeyFilters()</code>	Returns a list of the configured problem suppression filters. For example: <code>getProblemKeyFilters()</code>
Operation: <code>getProblemKeyFilter(filterID)</code>	Returns the filter pattern associated with the specified ID. For example: <code>getProblemKeyFilter(id)</code> To find the ID, use the <code>getProblemKeyFilters()</code> operation.
Operation: <code>removeProblemKeyFilter(filterID)</code>	Removes the filter pattern associated with the given filter ID. For example: <code>removeProblemKeyFilter(id)</code>

To configure a problem suppression filter:

1. From the WebLogic Domain menu, choose **System MBean Browser**.
The System MBean Browser page is displayed.
2. Expand **Application Defined Beans**, then **oracle.dfw**, then **domain.domain_name**, then **dfw.jmx.DiagnosticsConfigMBean**.
3. Select one of the **DiagnosticConfig** entries. There is one `DiagnosticConfig` entry for each server.
4. In the Application Defined MBeans pane, select the Operations tab.

5. Click **addProblemKeyFilter**. The Operation: addProblemKeyFilter page is displayed, as shown in the following figure:

Operation: addProblemKeyFilter Invoke Revert Return

Information
 The changes made on this mbean are not managed by the configuration session. The changes will be applied immediately. You cannot undo the changes from the Change Center.

MBean Name oracle.dfw:name=DiagnosticsConfig,type=oracle.dfw:jmx.DiagnosticsConfigMBean,ServerName=soa_server2
 Operation Name addProblemKeyFilter
 Description Adds a new Problem Key filter, with the specified filter pattern (i.e. SOA-4500.*), returning an id for the added filter
 Return Type java.lang.String

Parameters

Name	Type	Value
p1	java.lang.String	<input type="text"/>

Return Value

6. For **Value**, enter a regular expression that represents a pattern that you want to match pattern. For example, in a development environment, you might want to add a filter so that incidents are not created when java.lang.IllegalStateException Java Exceptions are reported. In that case, enter the following:

```
".* [java.lang.IllegalStateException] . *"
```

7. Click **Invoke**.
8. Click **Return** to return to the Application Defined MBeans page.

You can delete the filters using the removeProblemKeyFilter operation.

You can retrieve a specific filter, passing the ID of the filter to the getProblemKeyFilter operation.

Alternatively, you can retrieve a list of the filters using the getProblemKeyFilters attribute:

1. From the WebLogic Domain menu, choose **System MBean Browser**.
The System MBean Browser page is displayed.
2. Expand **Application Defined Beans**, then **oracle.dfw**, then **domain.domain_name**, then **dfw.jmx.DiagnosticsConfigMBean**.
3. Select one of the **DiagnosticConfig** entries. There is one DiagnosticConfig entry for each server.
4. In the Application Defined MBeans pane, select the Attributes tab.
5. Click **ProblemKeyFilters**.

The list of problem suppression filters is displayed.

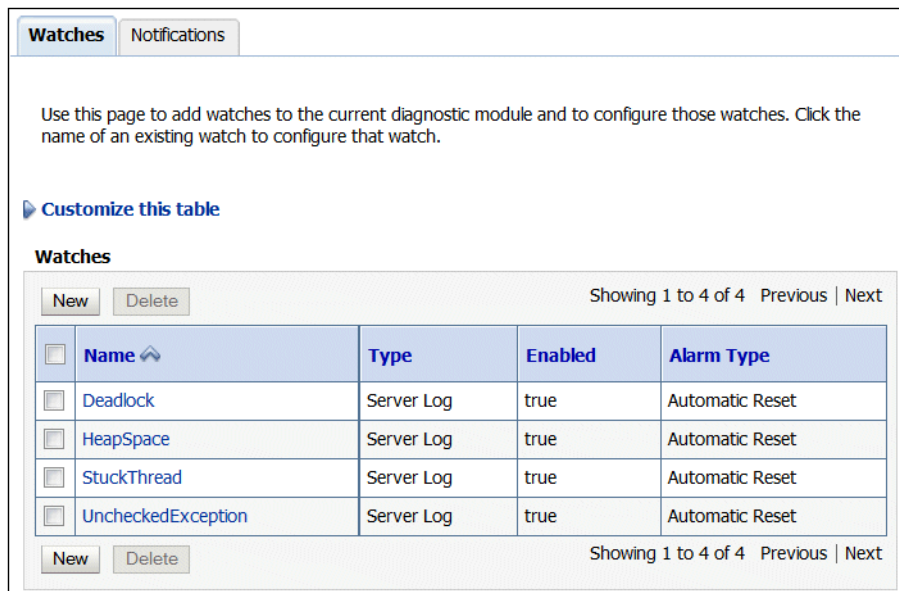
13.3.4 Configuring WLDF Watch and Notification for the Diagnostic Framework

Oracle Fusion Middleware configures a WLDF Diagnostics Module that contains a set of Watch and Notification rules for detecting a specific set of critical errors and creating an incident for each occurrence of those errors. The module is called Module-FMWDFW and contains the following set of Watch conditions:

Name	Description
Deadlock	Two or more Java threads have circular lock chains among their Java Monitor object usage.
StuckThread	An Oracle WebLogic Server ExecuteThread, which is blocked or busy for more than the time specified by the Oracle WebLogic Server StuckThreadMaxTime parameter.
UncheckedException	This category includes all Unchecked Exception, RuntimeException, and Errors caught by the Oracle WebLogic Server ExecuteThread, such as NullPointerException, StackOverflowError, or OutOfMemoryError.

The Diagnostic Module also includes a configured WLDF JMX Notification FMWDFW-notification of type `oracle.dfw.wldfnotification`. You can reuse this WLDF JMX Notification for your own WLDF Watch conditions to create an incident:

1. Display the Administration Console, as described in [Section 2.3.1](#).
2. In the left pane, expand **Diagnostics** and select **Diagnostic Modules**.
The Summary of Diagnostic Modules page is displayed.
3. Click **Module-FMWDFW**.
The Settings for Module-FMWDFW page is displayed.
4. Select the Watches and Notifications tab. The following figure shows the Watches and Notifications section:



5. Select the Watches tab and click **New**.
The Create Watch page is displayed.
6. For **Watch Name**, enter a name for the watch.
You can enter any name. Alternatively, you can use the following format to force the Diagnostic Framework to use a custom message ID:

`message-id#[application_name]#any_text`

The message ID consists of a prefix that can be 1 to 6 characters, and a number, that can be 1 to 6 digits. The application name is optional. For example:

```
WLS-40500#My_Watch_Name
```

The following example uses the application name testapp:

```
WLS-40501#testapp#My_Watch_Name
```

The Diagnostic Framework uses the message ID as the incident message ID in constructing the incident problem key.

7. For **Watch Type**, select a type, for example, Server Log.
8. Click **Next**.
9. For **Current Watch Rule**, construct an expression. For example, to construct the expression (SEVERITY = 'Error') AND (MSGID = 'BEA-000337'):
 - a. Click **Add Expressions**.
 - b. For **Message Attribute**, select Severity.
 - c. For **Operator**, select =.
 - d. For **Value**, enter ERROR.
 - e. Click **OK**.
 - f. Click **Add Expressions**.
 - g. For **Message Attribute**, select MSGID.
 - h. For **Operator**, select =.
 - i. For **Value**, enter BEA-000337.
 - j. Click **OK**.
 - k. In the Create Watch page, ensure that the operator selected is **AND**.
10. Click **Next**.
11. Select an alarm type and click **NEXT**.
12. For **Notifications**, select **FMWDFW-notification** and move it to the Chosen box.
13. Click **Finish**.

For more information on creating watches, see "Construct watch rule expressions" in the *Oracle WebLogic Server Administration Console Online Help*.

13.4 Investigating, Reporting, and Solving a Problem

This section describes how to use WLST and ADRCI commands and Remote Diagnostic Agent (RDA) to investigate and report a problem (critical error), and in some cases, resolve the problem. The section begins with a roadmap that summarizes the typical set of tasks that you must perform. It describes the following topics:

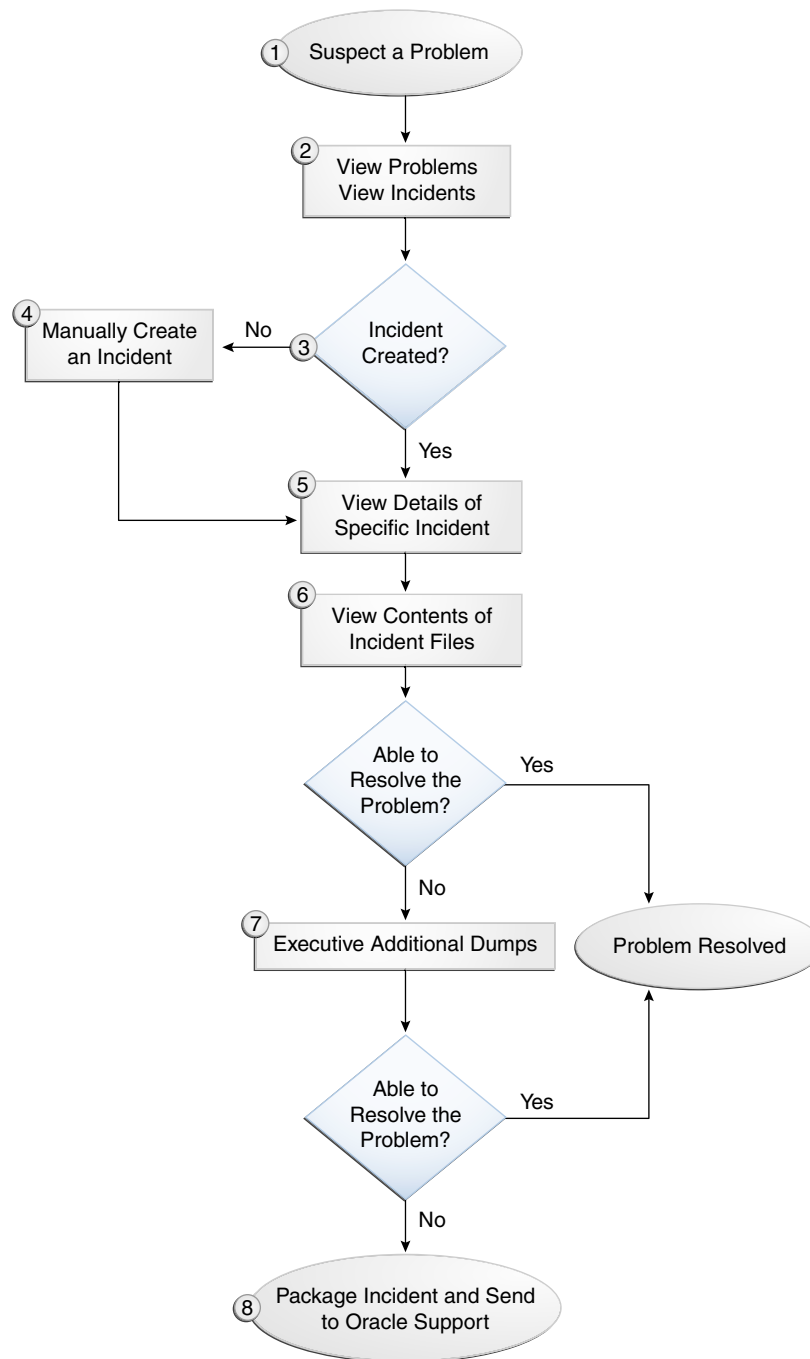
- [Roadmap—Investigating, Reporting, and Resolving a Problem](#)
- [Viewing Problems and Incidents](#)
- [Analyzing Specific Problem Keys](#)
- [Working with Diagnostic Dumps](#)
- [Configuring and Using Diagnostic Dump Sampling](#)

- [Managing Incidents](#)
- [Generating an RDA Report](#)

13.4.1 Roadmap—Investigating, Reporting, and Resolving a Problem

Typically, investigating, reporting, and resolving a problem begins with a critical error. This section provides an overview of that workflow.

[Figure 13-4](#) illustrates the tasks that you complete to investigate, report, and resolve a problem.

Figure 13–4 Flow for Investigating a Problem

The following describes the workflow illustrated in [Figure 13–4](#):

1. You notice that the system, component, or application is not functioning as expected. For example, you notice that there is a performance problem or users have reported that the application that they are trying to access is reporting errors.
2. Check to see if a problem and an incident have been created that may be related to the symptoms you are observing:
 - a. View the set of problems by using the WLST `listProblems` command, as described in [Section 13.4.2.1](#).

13.4.2.2 Viewing Incidents

You can list of all available incidents or the incidents related to a specific problem by executing the WLST `listIncidents` command, using the following format:

```
listIncidents([id], [ADRHome])
```

For example, to see the list of all incidents, use the following command:

```
listIncidents()
Incident Id      Incident Time                Problem Key
      2      Fri Mar 28 11:05:59 PDT 2014  MDS-50500 [MANUAL]
      1      Fri Mar 28 11:02:22 PDT 2014  MDS-50500 [MANUAL]
```

To view the incidents related to a specific problem, use the following command:

```
listIncidents(id='1')
Incident Id      Incident Time                Problem Key
      2      Fri Mar 28 11:05:59 PDT 2014  MDS-50500 [MANUAL]
      1      Fri Mar 28 11:02:22 PDT 2014  MDS-50500 [MANUAL]
```

To view the details of a particular incident, use the WLST `showIncident` command, using the following format:

```
showIncident(id, [adrHome] [,server])
```

For example, to see the details of incident 1, use the following command:

```
showIncident(id='1')
Incident Id: 1
Problem Id: 1
Problem Key: MDS-50500 [MANUAL]
Incident Time: Fri Mar 28 11:02:22 PDT 2014
Error Message Id: MDS-50500
Execution Context:
Flood Controlled: false
Dump Files :
  readme.txt
  jvm_threads10_i1.txt
  dms_metrics11_i1.txt
  dfw_samplingArchive13_i1.JVMThreadDump.txt
  dfw_samplingArchive13_i1.readme.txt
  odl_logs14_i1.txt
```

To view the contents of a file in the incident, use the WLST `getIncidentFile` command, using the following format:

```
getIncidentFile(id, name [,outputFile] [,adrHome] [,server])
```

For example, to view the contents for the file `odl_logs4_i1.dmp` use the following command:

```
getIncidentFile(id='1', name='odl_logs14_i1.txt',outputFile='/tmp/odl_logs4_i1_
dmp.output')
```

The command writes the output to the file `odl_logs4_i1_dmp.output`.

13.4.2.3 Querying Incidents

While the `listIncidents` command shows you the incidents related to a particular problem ID, or for a particular server, it does not allow you to restrict the list further. The WLST `queryIncidents` command lets you query for the value of particular

attributes across one or more servers, or all servers in a domain. For example, you can query by the time of incident creation or the ECID.

An expression contains an incident attribute, an operator, and a string, in the following format:

```
attribute operator "string"
```

You can combine query expressions with the Boolean operators AND or OR, and group them by parentheses ().

The following incident attributes are supported:

- **TIMESTAMP**: Incident creation time. You can use the `from` and `to` operators to specify a time range. The date format is `YYYY-MM-DD HH:MM`.
- **ECID**: Execution Context ID
- **PROBLEM_KEY**: Problem Key
- **MSG_FACILITY**: The error message facility, such as ORA or OHS.
- **MSG_NUMBER**: The error message ID, such as 600.

Custom incident attributes are also supported. For example, `TRACEID`, `APP`, `URI`, and `DSID` are supported. In addition, the context values, as shown in the incident `readme.txt` file, are supported. For example, `DFW_APP_NAME` and `DFW_USER_NAME` are supported.

The following operators are supported:

- `equals`
- `notEqual`
- `startsWith`
- `endsWith`
- `contains`
- `isNull`
- `notNull`

For example, you can query all incidents in all servers in the domain for the ECID `f19wAgN000001`:

```
queryIncidents(query="ECID equals f19wAgN000001")
```

The following example queries all incidents that occurred between March 1, 2014 and March 15, 2014, for the server `wls_server_1`:

```
queryIncidents(query="TIMESTAMP from '2014-03-01 00:00' AND TIMESTAMP to  
'2014-03-15 00:00'",  
servers=["wls_server_1"])
```

For more information about this command, see `queryIncidents` in the *WLST Command Reference for Infrastructure Components*.

13.4.3 Analyzing Specific Problem Keys

The Diagnostic Framework provides a set of well-defined problem keys for unhandled exceptions. These exceptions are either detected through the existing WLDF Watch "UncheckedException" or through the Diagnostic Framework `java.lang.Thread.UncaughtExceptionHandler` handler. Previously, the Diagnostic

Framework generated problem keys with different formats for the same type of issues. [Table 13–6](#) describes these problem keys and how to use them to investigate a problem.

Table 13–6 Uncaught Exception Problem Keys

Exception	Problem Key	Description
java.lang.OutOfMemoryError	DFW-99997 [java.lang.OutOfMemoryError]	Used by all java.lang.OutOfMemoryError incidents. With each incident of this type, a jvm.classhistogram dump is executed. The dump captures statistics about the instances of classes that have been loaded and the counts of associated Objects. Review the contents of this dump for a good starting point for understanding what has been loaded into the JVM's memory. In addition, the dms.metrics dump records statistics about the overall JVM memory.
java.sql.SQLException	DFW-99996 [ora-code java.sql.SQLException] [package.class.method][app-name]	Used for all exceptions of type java.sql.SQLException, including its subclasses. The Diagnostic Framework attempts to extract the Oracle error code from the exception error message, and if it is successful, uses that in the problem key. If not, it uses the exception name. Review the text associated with the exception to get more details, such as the operation that could not be performed on the database. In addition, you can review the SQL error code details for additional information.
All others	DFW-99998 [exception-name][package.class.name] [app-name]	Used by all other types of exceptions, such as java.lang.NullPointerException, java.io.IOException, java.lang.StringIndexOutOfBoundsException, that are not handled in a unique way. Review the text associated with the exception to get more details, such as the reason for the failure. The source line in the problem key is a best-attempt indicator of the location of the failure.

13.4.4 Working with Diagnostic Dumps

If you suspect a problem, you can make use of the built-in diagnostic dumps to report detailed diagnostics that can help diagnose the problem. Diagnostic dumps provide a means to output and record diagnostics data which serve as valuable information when diagnosing issues with Oracle Fusion Middleware components, applications, and infrastructure. The output from these dumps is intended to be used by customers and Oracle Support to diagnose issues with Oracle Fusion Middleware.

Diagnostic dumps are executed in the following ways:

- Manually, using WLST commands, as described in the following sections
For example, if your Java EE application is hanging and you suspect a deadlock, you could use the jvm.threads dump to obtain the set of threads.
- Automatically, when the Diagnostic Framework detects a critical error and creates an incident or when the administrator creates an incident

13.4.4.1 Listing Diagnostic Dumps

You can find a list of diagnostic dumps that are available for a Managed Server by executing the WLST `listDumps` command, using the following format:

```
listDumps([appName] [,server])
```

For example, to list the available dumps for `wls_server1`:

```
listDumps(server='wls_server1')
Location changed to domainRuntime tree. This is a read-only tree with DomainMBean
as the root.
For more help, use help(domainRuntime)
dfw.samplingArchive
dms.configuration
dms.ecidctx
dms.metrics
http.requests
jvm.classshistogram
jvm.threads
mds.MDSInstancesDump
odl.activeLogConfig
odl.logs
odl.quicktrace
opss.diagTest
opss.identityStoreUserRoleApiConfig
opss.securityContext
wls.image
```

Use the command `describeDump(name=<dumpName>)` for help on a specific dump.

[Table 13–7](#) lists the diagnostic dump actions that are defined by Oracle Fusion Middleware and their descriptions.

Table 13–7 Diagnostic Dump Actions

Dump Action	Description
<code>dms.ecidctx</code>	The data associated with a specific Execution Context ID (ECID), if specified. Otherwise, the data associated with all available ECIDs.
<code>dms.metrics</code>	Dynamic Monitoring Service (DMS) metrics. For information about these metrics, see "About Dynamic Monitoring Service (DMS)" in <i>Tuning Performance</i> .
<code>http.requests</code>	A summary of the currently active HTTP requests.
<code>jvm.classshistogram</code>	A JVM class histogram, the output of which varies depending on the JVM vendor.
<code>jvm.flightRecording</code>	The active JRockit Flight Recorder recording.
<code>jvm.threads</code>	Summary statistics about the threads running in a JVM as well as performing a full thread dump.
<code>mds.MDSInstancesDump</code>	Information about each MDS instance in the current JVM.
<code>odl.activeLogConfig</code>	The active Java logging configuration.
<code>odl.logs</code>	Contents of diagnostic logs, correlated by ECID or time range.
<code>odl.quicktrace</code>	Quick trace messages.
<code>wls.image</code>	The WLDF server image dump.

In addition, Oracle SOA Suite provides diagnostic dumps, as described in "Diagnosing Problems with SOA Composite Applications" in *Administering Oracle SOA Suite and Oracle Business Process Management Suite*.

13.4.4.2 Viewing a Description of a Diagnostic Dump

You can view a description of a particular dump, including the syntax for executing the dump by using the WLST `describeDump` command. You specify the name of the dump in which you are interested. For example, to view a description of the `dms.metrics` dump, use the following command:

```
describeDump(name='dms.metrics')
Name: dms.metrics
Description: Dumps DMS (Dynamic Monitoring Service) metrics.
Run Mode: asynchronous
Mandatory Arguments:
Optional Arguments:
  Name      Type      Description
  dump      STRING   How much to dump
  servers   STRING   Server names
  names     STRING   Name of DMS noun or metric
  format    STRING   Format of the dump output; raw or xml
  nountypes STRING   Type of DMS noun
```

13.4.4.3 Executing Dumps

If you detect a problem and want to gather additional diagnostic data, you can invoke the `executeDump` command for a specified dump. Each dump may have mandatory or optional arguments, or both. To view the arguments for a particular dump and how to specify them, use the `describeDump` command, as described in [Section 13.4.4.2](#).

The following example executes the dump with the name `dms.metrics` and the incident ID 1 and writes it to the file `dumpout.txt`:

```
executeDump(name='dms.metrics', outputFile='/tmp/dumpout.txt', id='1')
Dump file dms_metrics1_i1.dmp added to incident 1
```

The command writes the dump output to the information about incident 1. If you execute the `showIncident` command for incident 1, the output includes `dms_metrics1_i1.dmp`.

13.4.5 Configuring and Using Diagnostic Dump Sampling

Diagnostic dump sampling captures the output of diagnostic dumps at specified intervals. By sampling at regular intervals, diagnostic dump sampling can help to reveal issues such as slow running web requests, and where work is being performed in those requests.

This section contains the following topics:

- [Understanding Diagnostic Dump Sampling](#)
- [Configuring Dump Sampling](#)
- [Listing Dump Samplings](#)
- [Retrieving the Dump Sampling Output](#)

13.4.5.1 Understanding Diagnostic Dump Sampling

All diagnostic dump samplings are performed in the background, at specified intervals. By default, `jvm.threads` and `jvm.classhistogram` dumps are configured for

sampling. However, they are not active until an incident is generated. Then, they remain active for 72 hours, by default.

You can modify the settings for the default dump samplings and you can create new sampling definitions for the dump actions listed in [Table 13-7](#) and for any application-specific dumps. You can configure multiple sampling definitions for the same diagnostic dump, specifying different settings, such as sampling interval or server.

For each diagnostic dump sampling, the Diagnostic Framework stores the specified number of samples. When that limit is reached, the oldest sample is purged. All samples are purged when the server shuts down.

[Table 13-8](#) shows the settings of the dump samplings that are configured by default.

Table 13-8 Default Diagnostic Dump Samplings Configuration

Dump Name	Sampling Interval	Maximum Samples Stored
jvm.threads	60 seconds	10
jvm.classhistogram	30 minutes	5

The Diagnostic Framework triggers the retrieval of the dump samples whenever an incident is created (through error detection or manual incident creation.) In addition, you can retrieve the contents of the dump samples, as described in [Section 13.4.5.4](#).

You can retrieve the dump sample archives in either text or zip files:

- Text:** By default, the diagnostic dump samples are concatenated into a single archive file, in text format. An ASCII header and footer are wrapped around each sample in the archive file. The header contains a timestamp and the name of the diagnostic dump that produced the sample. Both the header and footer contain the number of the samples in the archive and the number of the particular sample. For example:

```

$$$=== BEGIN OF Diagnostic Dump - jvm.classhistogram (Archive #0 1_of_2) ===$$$
Fri Sep 07 07:00:00 PDT 2013

<text of dump sampling>

$$$=== END OF Diagnostic Dump - jvm.classhistogram (Archive #0 1_of_2) ===$$$

```

- Zip:** You can configure diagnostic dump samplings to return a zip file instead of a concatenated file. The zip file contains all available dump sample files. This format supports any diagnostic dumps whose outputs are in binary format not suitable for concatenation, as well as for dumps that generate output in text format. This format also reduces the size of the archive containing the samples.

The following example shows the contents of a zip file:

```

unzip -l jvm_dump.zip
Archive:  jvm_dump.zip
  Length   Date   Time    Name
  -----  ----  ----  -
    508780  08-21-13  07:25  dfw_
samplingArchive1065570966467923683.JVMThreadDump.dmp
     840   08-21-13  07:25  dfw_samplingArchive7749640004639161119.readme.txt
  -----  ----  ----  -
    509620                               2 files

```

In addition to a text or zip file, when you retrieve a dump sample, the Diagnostic Framework generates a readme file. The readme file either lists the line numbers for each dump sample in the archive (for text format) or the individual sample file names (for zip format). It also lists the timestamp for each sample and the index for the archive.

The dump sample files are named using the following format:

```
dfw_dumpArchivennn.Sampling_Name.{txt|zip}
```

In the format *nnn* is a unique number assigned by the Diagnostic Framework.

For example, the following is an example of the name of a dump sample file for JVMThreadDump:

```
dfw_dumpArchive17394218037.JVMThreadDump.txt
```

The readme files are named using the following format:

```
dfw_dumpArchivennn.readme.txt
```

In the format *nnn* is a unique number assigned by the Diagnostic Framework.

All samplings are scheduled to begin at the next nearest interval, corresponding to the frequency. For example, if a sampling is configured at 12:05:13 PM and the frequency is 5 seconds, the sample will be collected at 12:05:15 PM. This ensures that the collection of a series of samplings with the same frequency will occur at the same time. It also aligns all samples across machines, assuming their system clocks are synchronized.

Note: You must be connected to the Administration Server to execute the WLST dump sampling commands.

13.4.5.2 Configuring Dump Sampling

You can create additional dump samplings, update existing dump samplings, remove dump samplings and enable or disable dump sampling, as described in the following topics:

- [Activating the Default Samples](#)
- [Creating Dump Samplings](#)
- [Modifying Dump Sampling Settings](#)
- [Removing Dump Samplings](#)
- [Enabling or Disabling All Dump Sampling](#)

13.4.5.2.1 Activating the Default Samples By default the `jvm.threads` and `jvm.classhistogram` dumps are not activated until an incident occurs. Then, they are active for 72 hours, by default.

You can change the behavior so that the dumps are active even if an incident has not occurred by setting the value of the MBean `DumpSamplingIdleWhenHealthy` to `false`.

To change the amount of time used for determining the system's health, change the value of the `DumpSamplingMinimumHealthyPeriod` MBean.

For information about changing the value of the Diagnostic Framework MBeans, see [Section 13.3.1](#)

13.4.5.2.2 Creating Dump Samplings You can create dump samplings for any dump listed in [Table 13-7](#) and for any application-specific dumps. To create dump samplings, use the WLST command `addDumpSample`. The `addDumpSample` command uses the following syntax:

```
addDumpSample(sampleName="sample_name", diagnosticDumpName="dump_name",
  [appName="application_name",] samplingInterval=num_seconds,
  rotationCount=num_samples, [dumpedImplicitly={true|false},]
  [toAppend={true|false},] [args={"arg_name" : "value"},]
  [server="server_name"])
```

For example, to create a dump sampling for the `http.requests` dump, setting the sampling interval to 300 seconds and the rotation count to 10 samples, for the server `wls_server1`:

```
addDumpSample(sampleName="HTTPSampling", diagnosticDumpName="http.requests",
  samplingInterval=300, rotationCount=10, server="wls_server1")
```

HTTPSampling is added

For complete syntax, see "addDumpSample" in the *WLST Command Reference for Infrastructure Components*.

13.4.5.2.3 Modifying Dump Sampling Settings You can change the settings of existing dump samplings by using the WLST command `updateDumpSample`. The `updateDumpSample` command uses the following syntax:

```
updateDumpSample(sampleName="sample_name",
  [      appName="application_name",] samplingInterval=num_seconds,
      rotationCount=num_samples, [dumpedImplicitly={true|false},]
  [      toAppend={true|false},] [args={"arg_name" : "value"},]
  [      server="server_name"])
```

For example, to modify the dump sampling `HTTPSampling`, changing the sampling interval to 200 and the rotation count to 5:

```
updateDumpSample(sampleName="HTTPSampling", samplingInterval=200,
  rotationCount=5, server="wls_server1")
```

HTTPSampling is updated

For complete syntax, see "updateDumpSample" in the *WLST Command Reference for Infrastructure Components*.

13.4.5.2.4 Removing Dump Samplings You can remove existing dump samplings using the WLST command `removeDumpSample`. The `removeDumpSample` command uses the following syntax:

```
removeDumpSample(sampleName="sample_name", [server="server_name"])
```

For example, to remove the dump sampling `HTTPSampling`:

```
removeDumpSample(sampleName="HTTPSampling", server="wls_server1")
```

Removed HTTPSampling

For complete syntax, see "removeDumpSample" in the *WLST Command Reference for Infrastructure Components*.

13.4.5.2.5 Enabling or Disabling All Dump Sampling

You can enable or disable all dump sampling using the WLST command `enableDumpSampling`. This command affects all configured dump samplings. The `enableDumpSampling` command uses the following syntax:

```
enableDumpSampling(enable={true|false}, [server="server_name"])
```

Note that the server parameter is valid only if you are connected to the Administration Server. If you do not specify the server parameter, dump sampling is disabled for the Administration Server.

For example, to disable dump sampling for the Administration Server:

```
enableDumpSampling(enable=false)
```

```
Dump sampling disabled
```

To determine if dump sampling is enabled or disabled, use the WLST command `isDumpSamplingEnabled`. The `isDumpSamplingEnabled` command uses the following format:

```
isDumpSamplingEnabled([server="server_name"])
```

For complete syntax, see "enableDumpSampling" and "isDumpSamplingEnabled" in the *WLST Command Reference for Infrastructure Components*.

13.4.5.3 Listing Dump Samplings

You can list dump samplings using the WLST command `listDumpSamples`. You can list all dump samplings, a specified dump sampling, or all dump samplings associated with a specified server. The `listDumpSamples` command uses the following syntax:

```
listDumpSample([sampleName="sample_name"], [server="server_name"])
```

For example, to list all dump samplings associated with the server `wls_server1`:

```
listDumpSamples(server="wls_server1")
Name           : JVMThreadDump
Dump Name      : jvm.threads
Application Name :
Sampling Interval : 30
Rotation Count : 20
Dump Implicitly : true
Append Samples : true
Dump Arguments : context=true, timing=true, progressive=true, depth=20,
threshold=30000
```

```
Name           : JavaClassHistogram
Dump Name      : jvm.classshistogram
Application Name :
Sampling Interval : 1800
Rotation Count : 5
Dump Implicitly : false
Append Samples : true
Dump Arguments :
```

For complete syntax, see "listDumpSample" in the *WLST Command Reference for Infrastructure Components*.

13.4.5.4 Retrieving the Dump Sampling Output

To retrieve the output of dump samples, you can use the WLST `executeDump` command or the WLST `getSamplingArchives` command, as described in the following topics:

- [Retrieving Dump Samples Using the `executeDump` Command](#)
- [Retrieving Dump Samples Using the `getSamplingArchives` Command](#)

13.4.5.4.1 Retrieving Dump Samples Using the `executeDump` Command You can retrieve dump samples using the WLST `executeDump` command, specifying the `dfw.samplingArchive` dump. This command collects all default sample archives and any dump samples that are specified with the parameter `dumpImplicitly=true` from a temporary location and concatenates them into a single file. The command also returns a readme file, with details of the dump samples.

When you use the `executeDump` command, you use the following syntax:

```
executeDump (name="dfw.samplingArchive", outputFile="filename")
```

For the `outputFile` parameter, you can specify a text file or a zip file. If you specify a zip file, you must use the argument `zipOutput=true`.

For any dump sampling that is configured with the parameter `dumpImplicitly=false`, you must specify the optional `dfw.samplingArchive` argument `sampleName` to collect the contents of those dump samples. For example:

```
executeDump (name='dfw.samplingArchive', args={'sampleName' :
'JavaClassHistogram'})
```

For more information, see "`executeDump`" in the *WLST Command Reference for Infrastructure Components*.

13.4.5.4.2 Retrieving Dump Samples Using the `getSamplingArchives` Command You can retrieve dump samples using the WLST `getSamplingArchives` command. This command collects all dump samples in a zip file containing the individual dump sample files and a readme file. This method is particularly useful in dealing with binary format dumps.

The `getSamplingArchives` command uses the following syntax:

```
getSamplingArchives ([sampleName="sample_name"] [, outputFile="filename"]
[, server="server_name"])
```

For example to retrieve the dump samples for the sampling `JavaClassHistogram`, use the following command:

```
getSamplingArchives (sampleName="JavaClassHistogram",
outputFile="/tmp/sampling.zip")
```

The following shows the contents of the zip file:

```
unzip -l /tmp/sampling.zip
Archive:  /tmp/sampling.zip
  Length      Date    Time    Name
-----
 6241768  04-27-13  11:19   dfw_
samplingArchive8680976839106379444.JavaClassHistogram.dmp
    552  04-27-13  11:19   dfw_samplingArchive7861027727509995202.readme.txt
-----
 6242320                                2 files
```

For complete syntax, see "getSamplingArchives" in the *WLST Command Reference for Infrastructure Components*.

13.4.6 Managing Incidents

The Diagnostic Framework stores incidents, whether they are created automatically or manually, and Oracle Fusion Middleware provides tools to help you process incident reports and to package those incidents to send to Oracle Support. The following sections describe:

- [Creating an Incident Manually](#)
- [Creating an Aggregated Incident](#)
- [Packaging an Incident](#)
- [Generating an RDA Report](#)
- [Purging Incidents](#)

13.4.6.1 Creating an Incident Manually

System-generated problems—critical errors generated internally—are automatically added to the Automatic Diagnostic Repository (ADR). You can gather additional diagnostic data on these problems, upload diagnostic data to Oracle Support, and in some cases, resolve the problems, all with the workflow that is explained in [Section 13.4](#).

Consider creating an incident manually when you encounter an issue, such as software failure or performance problem and you want to gather more diagnostic data, but the Diagnostic Framework has not automatically created an incident.

You use the WLST command `createIncident` to create an incident manually. You can specify an incident based on time, a message ID, an impact area, or an ECID. Then, you can inspect the content of the incident or send it to Oracle Support for further analysis.

For example, to manually create an incident based on a message ID:

1. Search the log files, as described in [Section 12.3.2](#). If you find a message that you suspect is related to the issue you are seeing, you can use the message ID when you create the incident.
2. Use the following commands to invoke WLST, connect to the Managed Server and navigate to the Managed Server instance:

```
java weblogic.WLST
connect('username', 'password', 'localhost:7001')
cd('servers/server_name')
```

3. Create the incident, using the `createIncident` command, with the following format:

```
createIncident([adrHome] [,incidentTime] [,messageId] [,ecid] [,appName]
[,description] [,server])
```

For example, to create an incident based on the error with the message ID MDS-50500, use the following command, specifying the message ID, and provide a description of the incident to help you and Oracle support track the incident:

```
createIncident(messageId='MDS-50500', description='sample incident')
Incident Id: 1
Problem Id: 1
```

```
Problem Key: MDS-50500 [MANUAL]
Incident Time: Fri Mar 28 11:02:22 PDT 2014
Error Message Id: MDS-50500
Execution Context: null
Flood Controlled: false
Dump Files :
  jvm_threads10_i1.txt
  dms_metrics11_i1.txt
  dfw_samplingArchive13_i1.JVMThreadDump.txt
  dfw_samplingArchive13_i1.readme.txt
  odl_logs14_i1.txt
```

If you do not specify a server, the incident collects information from the server to which you are connected. To specify a server, use the `server` option, as shown in the following example:

```
createIncident(messageId='MDS-50500', description='sample incident',
server='wls_server1')
)
```

If you do not specify the `adrHome` option, the incident is created in the server to which you are connected. For example, if you are connected to the Administration Server, the incident is created in the `adrHome` for the Administration Server.

The Diagnostic Framework evaluates the command and invokes the appropriate diagnostic dumps. The incident and the diagnostic dumps are written to the ADR. Each diagnostic dump writes its output to the incident.

You can view the information about the incident, as described in [Section 13.4.2.2](#).

You can view the information in the dumps, as described in [Section 13.4.4](#).

13.4.6.2 Creating an Aggregated Incident

If you have several incidents and want to combine them into a single incident, you can use the WLST `createAggregatedIncident` command. For example, if you used selective tracing, the resulting incidents containing the trace data may be generated on multiple servers. With the `createAggregatedIncident` command, you can generate an aggregated incident that meets criteria you specify. The original incidents are untouched. That is, the aggregated incident contains a copy of the incident files from the queried incidents.

The aggregated incidents are created on the Administration Server host, but they can contain incidents from one or more servers or all servers in the domain.

You construct a query using an expression that contains an incident attribute, an operator, and a string, in the following format:

```
attribute operator "string"
```

You can combine query expressions with the Boolean operators AND or OR, and group them by parentheses ().

For information about the supported attributes and operators, see "createAggregatedIncident" in the *WLST Command Reference for Infrastructure Components*.

Each aggregated incident will contain a zip file for each incident returned from the query, as well as descriptive text detailing the query used and the details of each incident.

For example, to create an aggregated incident for all incidents that contain the `ODL_TRACE_ID` of 123456 on the server `wls_server1`:

```
createAggregatedIncident(query="ORDL_TRACE_ID equals 123456", servers="wls_
server1")
Incident 55 created, containing the following incidents:
Server wls_server1
Incident Id    Problem Key                                Incident Time
15            TRACE [123456] [MANUAL]                            Mon Apr 15 11:22:12 EDT 2014
```

To create an aggregated incident for all incidents that contain the ODL_TRACE_ID of 123456 on all servers in the domain:

```
createAggregatedIncident(query="ORDL_TRACE_ID equals 123456")
Incident 55 created, containing the following incidents:
Server wls_server1, wls_server2
Incident Id    Problem Key                                Incident Time
15            TRACE [123456] [MANUAL]                            Mon Apr 15 11:22:12 EDT 2014
```

13.4.6.3 Packaging an Incident

You can package the incident to facilitate sending the information to Oracle Support by using the ADR Command Interpreter (ADRCI). The ADRCI utility enables you to investigate and report problems in a command-line environment. With ADRCI, you can package incident and problem information into a zip file for transmission to Oracle Support.

The ADRCI command-line utility is located in the following directory:

```
(UNIX) ORACLE_HOME/oracle_common/adr
(Windows) ORACLE_HOME\oracle_common\adr
```

Packaging an incident involves a three-step process:

1. Create a logical package.

The package is denoted as logical because it exists only as metadata in the ADR. It has no content until you generate a physical package from the logical package. The logical package is assigned a package number, and you refer to it by that number in subsequent commands.

You can create the logical package as an empty package, or as a package based on an incident number, a problem number, a problem key, or a time interval. If you create the package as an empty package, you can add diagnostic information to it in step 2.

Creating a package based on an incident means including diagnostic data, such as dumps, for that incident. Creating a package based on a problem number or problem key means including in the package diagnostic data for incidents that reference that problem number or problem key. Creating a package based on a time interval means including diagnostic data on incidents that occurred in the time interval.

2. Add diagnostic information to the package.

If you created a logical package based on an incident number, a problem number, a problem key, or a time interval, this step is optional. You can add additional incidents to the package or you can add any file within the ADR to the package. If you created an empty package, you must use ADRCI commands to add incidents or files to the package.

3. Generate the physical package.

When you submit the command to generate the physical package, ADRCI gathers all required diagnostic files and adds them to a zip file in a designated directory.

You can generate a complete zip file or an incremental zip file. An incremental file contains all the diagnostic files that were added or changed since the last zip file was created for the same logical package. You can create incremental files only after you create a complete file, and you can create as many incremental files as you want. Each zip file is assigned a sequence number so that the files can be analyzed in the correct order.

Zip files are named according to the following format:

```
packageName_mode_sequence.zip
```

In the format:

- `packageName` consists of a portion of the problem key followed by a timestamp.
- `mode` is either `COM` or `INC`, for complete or incremental.
- `sequence` is an integer.

For example, to package an incident, take the following steps:

1. Set the `ORACLE_HOME` and `LD_LIBRARY_PATH` environment variables as shown in the following example:

```
ORACLE_HOME=ORACLE_HOME/oracle_common  
LD_LIBRARY_PATH=ORACLE_HOME/oracle_common/adr
```

2. Invoke `ADRCI`. For example:

```
ORACLE_HOME/oracle_common/adr/adrci
```

3. Use the `SET BASE` command to specify the ADR Base and the `SET HOMEPATH` command to specify the ADR home that contains the incident. The path for the `HOMEPATH` is relative to the ADR Base.

```
SET BASE /scratch/oracle/config/domains/wls_domain/servers/wls_server1/adr  
SET HOMEPATH diag/ofm/wls_domain/wls_server1
```

4. Generate the logical package:

```
IPS CREATE PACKAGE INCIDENT incident_number
```

For example, the following command creates a package based on incident 1:

```
IPS CREATE PACKAGE INCIDENT 1  
Created package 1 based on incident id 1, correlation level typical
```

`ADRCI` assigns the logical package a number.

5. Optionally, you can add diagnostic information to the logical package. You can add the following types of information:
 - All diagnostic information for a particular incident. For example, you can add another incident that you think might be related to the incident you are packaging, using the following command:

```
IPS ADD INCIDENT incident_number PACKAGE package_number
```

- A named file within the ADR. For example, if an incident is related to an application, you can add the `.ear` file for the application. You can also add a `readme` file with notes you provide to Oracle Support. For example, to add a file to the package, use the following command:

```
IPS ADD FILE filespec PACKAGE package_number
```

6. Generate the physical package using the following command:

```
IPS GENERATE PACKAGE package_number IN path
```

For example, to generate a package with the number 1, use the following command:

```
IPS GENERATE PACKAGE 1 in /tmp
Generated package 1 in file /tmp/BEA337Web_20100223132315_COM_1.zip, mode
complete
```

This generates a complete physical package (zip file) in the designated path.

For more information, see the "ADRCI: ADR Command Interpreter" chapter of the *Oracle Database Utilities*.

13.4.6.4 Purging Incidents

By default, incidents are purged when the total size of all incidents exceed 500 MB. You can use the `maxTotalIncidentSize` MBean parameter to change this value, as described in [Section 13.3.1](#).

You can manually purge incidents using the ADRCI command. You can purge based on an ID or range of IDs, the age of the incident, or the type of incident. For example, to purge incidents that are older than 60 minutes, use the following command:

```
purge -age 60
```

See the "ADRCI: ADR Command Interpreter" chapter of the *Oracle Database Utilities*.

13.4.7 Generating an RDA Report

You can use the Remote Diagnostic Agent (RDA), a command-line diagnostic tool, to provide a comprehensive picture of your environment. Additionally, RDA can provide recommendations on various topics, for example configuration and security. This aids you and Oracle Support in resolving issues.

RDA is a set of command line diagnostic scripts that are executed by an engine written in the Perl programming language. RDA is used to gather detailed information about an Oracle environment; the data gathered is in turn used to aid in problem diagnosis. The output is also useful for seeing the overall system configuration.

RDA is designed to be as unobtrusive as possible; it does not modify systems in any way. A security filter is provided if required.

RDA collects information that is useful for troubleshooting issues in the following areas:

- Installation and configuration
- Performance
- ORA-600, ORA-7445, ORA-3113, and ORA-4031 errors
- Upgrade, migration, and linking
- Oracle Database
- Oracle Fusion Middleware

To run RDA, execute the following:

```
(UNIX) ORACLE_HOME/oracle_common/rda/rda.sh
(Windows) ORACLE_HOME\oracle_common\rda\rda.cmd
```

The following shows a part of the output:

```
./rda.sh
-----
S000INI: Initializes the Data Collection
-----
RDA uses the output file prefix to identify all files belonging to the same
data collection. The prefix must start with a letter and must contain only
alphanumeric characters.

Enter the prefix to be used for all the generated files
Hit 'Return' to accept the default (RDA)
>

Enter the directory used for all the files to be generated
Hit 'Return' to accept the default
(/scratch/oracle1/Oracle/Middleware/Oracle_Home/oracle_common/rda/output)
>

Do you want to keep report packages from previous runs (Y/N)?
Hit 'Return' to accept the default (N)
>

Enter the Oracle home to be used for data analysis
Hit 'Return' to accept the default
(/scratch/oracle1/Oracle/Middleware/Oracle_Home
)
For more information about RDA, see the readme file, which is located at:

(UNIX) ORACLE_HOME/oracle_common/rda/README_Unix.txt
(Windows) ORACLE_HOME\oracle_common\rda\README_Windows.txt
```

13.5 Managing and Running the Health Test Framework

Oracle Fusion Middleware provides a Health Test Framework that includes diagnostic tests that are designed to exercise particular aspects of Oracle Fusion Middleware and its applications, to determine whether they are operating correctly and to help identify and resolve any problems.

This section contains the following topics:

- [Understanding the Health Test Framework](#)
- [Understanding the Health Test Framework File Repository](#)
- [Using the Health Test Framework Command Line](#)
- [Managing the Health Test Framework](#)
- [Running Health Test Framework Diagnostic Tests](#)
- [Searching for Health Test Framework Diagnostic Tests](#)
- [Retrieving a Description of a Health Test Framework Test](#)
- [Listing Health Test Framework Test Runs](#)
- [Generating Health Test Framework Reports](#)

13.5.1 Understanding the Health Test Framework

The Health Test Framework lets you execute diagnostic tests and collects the results into detailed diagnostic reports. The diagnostics tests are installed when you install or patch Oracle Fusion Middleware.

You can use the Health Test Framework to check normal system health and to troubleshoot system problems. You can configure your Oracle Fusion Middleware environment to run the diagnostic tests using the Health Test Framework command line interface.

A diagnostic test may or may not be associated with a particular error message. If an Oracle Fusion Middleware application handles a particular error in a way that triggers the creation of an incident, then any diagnostic tests that are associated with the error message for the incident run automatically. The test results are associated with the incident and the identity of the user who received the error message is recorded. The diagnostic tests and results are stored in file-based repository, as described in [Section 13.5.2](#).

13.5.2 Understanding the Health Test Framework File Repository

The Health Test Framework stores tests and test results in a file-based repository. The repository has two primary stores:

- TestDef, which contains test definitions, test metadata, data related to test parameters, language data files, and index files.
- Test Run, which contains data related to the test run and execution, report files, and index files.

Index files are used for improving the speed of searching and querying.

The repositories are created when you register tests or run tests if the repository does not exist at the specified location.

You can specify the location of the repository in the configuration properties file, `diagfsconfig.properties`. This file is located in:

```
ORACLE_HOME/diagbase/dtf_filestore
```

By default, the file stores are located in:

```
ORACLE_HOME/diagbase/dtf_filestore/testdef
ORACLE_HOME/diagbase/dtf_filestore/testrun
```

13.5.3 Using the Health Test Framework Command Line

The Health Test Framework provides two command line interfaces, `dfwhealthtestadminctl.sh` for administration commands and `dfwhealthtestctl.sh` for execution commands, as described in the following sections:

- [dfwhealthtestadminctl.sh Command Line](#)
- [dfwhealthtestctl.sh Command Line](#)

13.5.3.1 dfwhealthtestadminctl.sh Command Line

The Health Test Framework provides the `dfwhealthtestadminctl.sh` command line for administering the health tests. With it, you can register tests and rebuild the index.

Before you can run the `dfwhealthtestadmin.ctl` command, you must set the following environment variables:

- ORACLE_HOME: The Oracle home
- JAVA_HOME: The Java home
- dtf_fs_diagbase: The location of the repository

The dfwhealthtestadminctl.sh command-line interface is located in:

`ORACLE_HOME/oracle_common/common/bin`

The syntax of the command-line interface is:

`/dfwhealthtestadminctl.sh command [options]`

Table 13–9 lists the Health Test Framework administration commands:

Table 13–9 Health Test Framework dfwhealthtestadminctl.sh Commands

Command	Description
help	Provides command line help.
register	Registers one or more Health Test Framework test with the repository.
index	Rebuilds the index with the existing data files.

13.5.3.1.1 help Provides help for the commands.

The syntax is:

`help command`

The following table describes the parameters for the help command:

Parameter	Description
command	The name of the command.

13.5.3.1.2 register Registers one or more tests with the repository.

The syntax is:

```
register testfile=test_xml_files | dir=test_dirs
      [validateonly={Y|N}]
      testjar=jar_file_location
```

The following table describes the parameters for the register command:

Parameter	Description
testfile	One or more XML test files to register. Provide the path to the files, using a comma-separated list for more than one file.
dir	One or more directories to register. Provide the path to the directories, using a comma-separated list for more than one directory. Use this option to register multiple tests from the same directory.
validateonly	Optional. A Boolean value to specify whether to only validate the test or to upload the test or tests to the repository. Value values are Y (to only validate the test) or N (to upload the tests).
testjar	The location of the test jar files.

13.5.3.1.3 index Rebuilds the index for the testdef or testrun repository, using the data files in the repository.

The syntax is:

```
index [refresh={testdef|testrun}]
```

The following table describes the parameters for the index command:

Parameter	Description
refresh=testdef	Refreshes the index for the testdef repository.
refresh=testrun	Refreshes the index for the testrun repository.

13.5.3.2 dfwhealthtestctl.sh Command Line

The Health Test Framework provides the dfwhealthtestctl.sh command line for running the health tests. With it, you can run tests, list runs and tests, get a description of a test, get the status of tests, and retrieve a report of a test or test run.

The dfwhealthtestctl.sh command-line interface is located in:

```
ORACLE_HOME/oracle_common/common/bin
```

The syntax of the command-line interface is:

```
/dfwhealthtestctl.sh command [options]
```

Table 13–10 lists the Health Test Framework dfwhealthtestctl.sh commands:

Table 13–10 Health Test Framework dfwhealthtestctl.sh Commands

Command	Description
descstest	Provides a detailed description of a specified test.
listrun	List the test runs.
listtest	Lists the description of one or more tests.
report	Extract a report of a test run.
run	Run one or more tests.
status	Get the status of a test run or execution.

13.5.3.2.1 descstest Provides a detailed description of a specified test.

The syntax is:

```
descstest {testid=testid | testname=testname}
          [showparam={Y|N}]
```

The following table describes the parameters for the descstest command:

Parameter	Description
testid	The ID of the test. To obtain the ID, use the listtest command. You must specify either this parameter or the testname parameter.
testname	The name of the test. You must specify either this parameter or the testid parameter.
showparam	Optional. A Boolean value to specify whether to retrieve the parameters for the test. Value values are Y or N.

13.5.3.2.2 help Provides help for the commands.

The syntax is:

```
help command
```

The following table describes the parameters for the help command:

Parameter	Description
command	The name of the command.

13.5.3.2.3 listrun Retrieves summary information for the test runs. You can retrieve the information by run name, run status, start time, and test name.

The syntax is:

```
listrun { runname=runname | testname=testname | status=status | lasthours=hours }
        [showexec={Y|N}]
```

The following table describes the parameters for the listrun command:

Parameter	Description
runname	The name of the run for which you want to return results. To get the runname, use the listrun command without any parameters.
testname	The name of the test for which you want to return results.
status	The status of the run for which you want to return results. Valid values are running, warning and success.
lasthours	The number of hours for which you want to return results.
showexec	Optional. A Boolean value to specify whether to retrieve the execution of the tests. Value values are Y or N.

13.5.3.2.4 listtest Lists one or more tests. You can use wildcards to specify the names of the tests

The syntax is:

```
listtest [testname=testname]
        [productcode=productcode]
```

The following table describes the parameters for the help command:

Parameter	Description
testname	The names of one or more tests, in a comma-separated list. You can use wildcards to specify a pattern to match the names of tests.
productcode	The name of the product. You can use wildcards to specify a pattern to match the name of the product.

13.5.3.2.5 report Extract a test report for a particular test run or execution.

The syntax is:

```
report { runname=runname | runid=run_id | execid=execution_id }
        [destdir=destination_directory]
        [format=HTML | XML]
        [translate={Y | N}]
```

The following table describes the parameters for the report command:

Parameter	Description
runname	The name of the run. To get the name, use the listrun command. You must specify this parameter, <code>runid</code> , or <code>execid</code> .
runid	The ID of the run. To get the ID, use the listrun command. You must specify this parameter, <code>runname</code> , or <code>execid</code> .
execid	The execution ID of the run. To get the ID, use the listrun command. You must specify this parameter, <code>runname</code> , or <code>runid</code> .
destdir	Optional. The destination directory to which the report files are written. If not specified, the report files are extracted under the <code>java.io.tmpdir/user.name/diagfwk</code> directory, where <code>java.io.tmpdir</code> and <code>user.name</code> are Java system properties.
format	The format of the generated report. Valid values are HTML and XML.
translate	A Boolean value specifying whether to translate the report. Value values are Y or N.

13.5.3.2.6 run Run the specified tests.

```
run {test=testnames | productcode=codes }
    [runname=name]
    [runoption=asynch]
    [input:param1=value1 param2=value2 ...]
    [inputfile=filename]
    [contextfile=context_file]
    [moninterval=monitoring_interval]
    [nthreads=number_of_threads]
    [reportshowparam=show_param]
```

The following table describes the parameters for the run command:

Parameter	Description
test	The names of one or more tests, in a comma-separated list. If you specify a single test name, you can also specify one or more input parameter names and values using the input parameter. You must specify this parameter or the productcode parameter.
productcode	The code for one or more products that include the tests you want to run. Specify more than one product code in a comma-separated list.
runname	Optional. A name for the current run. If not specified, the command generates a default run name.
moninterval	The interval, in seconds, in which the status of the run is uploaded to the test repository. The default value is 30 seconds.
nthreads	The number of parallel threads that should be spawned to execute tests in this run. The default value is 5. Specifying a value of 1 for this parameter will execute the tests serially.
runoption	Optional. Options for running the tests. The valid value is <code>asynch</code> , which runs the test asynchronously in the background.

Parameter	Description
input	Optional. If you use this parameter, use one or more parameter name/value pairs. For example: domainhome=/scratch/oracle/domains/basedomain You can only use this parameter when you run only one test.
inputfile	The path to a file containing input parameters. The file should have each input name/value pair on a separate line. The format of each line is: <i>input_param_name: input_param_value</i>
contextfile	The path to a file that contains user system properties to be used at run time.
reportshowparam	Sets the input and output parameter display. By default all parameters are hidden during execution. To specify that the parameters are shown, use input or output, or a comma-separated string with both. For example: reportshowparam=input,output

13.5.3.2.7 status Get the status of a test run by specifying the run name, run ID, or execution ID.

The syntax is:

```
status { runname=runname | runid=run_id | execid=execution_id }
        [printtree={Y|N}]
```

The following table describes the parameters for the status command:

Parameter	Description
runname	The name of the run. To get the run name, use the listrun command.
runid	The ID of the run. To get the ID, use the listrun command.
execid	The execution ID of the run. To get the ID, use the listrun command.
printtree	Specifies whether to print the status of all nested conditions. Valid values are Y and N.

13.5.4 Managing the Health Test Framework

You can register tests and rebuild the index, as described in the following topics:

- [Creating a Repository and Registering Health Test Framework Tests](#)
- [Rebuilding the Health Test Framework Indexes](#)

13.5.4.1 Creating a Repository and Registering Health Test Framework Tests

To create a repository, you register a test using the `dfwhealthtestadminctl.sh register` command. The command creates a repository and registers one or more tests with the repository.

To create a repository and register the tests, take the following steps:

1. Set the `dtf_fs_diagbase` environment variable to specify the location of the repository. For example:

```
setenv dtf_fs_diagbase /scratch/Oracle/Middleware/diag
```

- Execute the following command, which creates the repository and registers one test in the repository:

```
dfwhealthtestadminctl.sh register testfile=/scratch/tests/sampleTest.xml
                             testjar=/scratch/tests/testjar
```

You can register more than one test at a time using the `testfile` or `dir` parameters:

- To register more than one test using the `testfile` parameter, you can use a comma-separated list or wildcards.

The following example registers two tests, using a comma-separated list:

```
dfwhealthtestadminctl.sh register testfile=/scratch/tests/sampleTest.xml,
                             /scratch/morettests/sampleTest.xml
                             testjar=/scratch/tests/testjar
```

The following example registers more than one test, using wildcards:

```
dfwhealthtestadminctl.sh register testfile=/scratch/tests/%Test.xml,
                             testjar=/scratch/tests/testjar
```

- To register more than one test using the `dir` parameter, you can specify one or more directories in a comma-separated list.

The following example registers all tests in the specified directory:

```
dfwhealthtestadminctl.sh register dir=/scratch/df_test
```

13.5.4.2 Rebuilding the Health Test Framework Indexes

Indexes improve the speed of searching and querying the Health Test Framework repository. Indexes related to test definition are stored in the `testdef` file store. Indexes related to test runs and execution are stored in the `testrun` file store.

In some circumstances, you may want to refresh the indexes. You use the `dfwhealthtestadminctl.sh index` command, specifying the `testdef` or `testrun` file store. The following example refreshes the `testdef` file store:

```
dfwhealthtestadminctl.sh index refresh=testdef
```

13.5.5 Running Health Test Framework Diagnostic Tests

You run the Health Test Framework diagnostic tests using the `dfwhealthtestctl.sh` command line interface, which is located in:

```
ORACLE_HOME/oracle_common/common/bin
```

To run a test, use the `run` command, using the format described in [Section 13.5.3.2.6](#). For example, to run the test `SampleTest`, use the following command:

```
./dfwhealthtestctl.sh command
                    [testfile=SampleTest.xml]
```

You can run one or more tests at the same time:

- To run one or more tests by specifying the test names in a comma-separated list:

```
./dfwhealthtestctl.sh run test=oracle.dfw.healthtest.test.sample.SampleTest2
Processing "run" command ...
```

```
Executing run ID "1340125981427" with name "TestRun_1340125981427" ...
sampleTest2 sleep for a while...
sampleTest2 done
```

Run ID "1340125981427" with name "TestRun_1340125981427" started at 3/21/2014 10:13:01 AM and completed at 3/21/2014 10:13:04 AM. No diagnostic issues were detected.

- To run one or more tests by using wildcards for the test name:

```
./dfwhealthtestctl.sh run test=oracle.dfw.healthtest.test.sample.SampleTest*
```
- To run all tests associated with a particular product:

```
./dfwhealthtestctl.sh run productcode=idm
```

If you are running only one test, you can specify input options either on the command line or in an input file:

- To specify the input options on the command line, use the `input :` parameter:

```
./dfwhealthtestctl.sh run
test=oracle.dfw.healthtest.test.sample.SampleTest,oracle.dfw.healthtest.test.sa
mple.SampleTest2
                                input:userid=11 input:roleid=22
```
- To specify the input options in an input file, create the file and specify it on the command line using the `inputfile` parameter. The following shows the format of the input file:

```
input_parameter1:parameter_value1
input_parameter2:parameter_value2
```

For example:

```
userid:11
roleid:22
```

Then, specify the file on the command line:

```
./dfwhealthtestctl.sh run test=oracle.dfw.healthtest.test.sample.SampleTest
                                inputfile=/tmp/inputfile
```

13.5.6 Searching for Health Test Framework Diagnostic Tests

You can search for tests or runs using the `dfwhealthtestctl.sh listtest` command. Optionally, you can specify the name of the test or product code:

- To search for all tests:

```
./dfwhealthtestctl.sh listtest
```
- To search for one test named `SampleTest`:

```
./dfwhealthtestctl.sh listtest testname=SampleTest
```
- To search for more than one test using wildcards:

```
./dfwhealthtestctl.sh listtest testname="S*"
```
- To search for all tests related to a particular product:

```
dfwhealthtestctl.sh listtest productcode=idm
```


13.5.7 Retrieving a Description of a Health Test Framework Test

You can retrieve the description of a specified test using the `dfwhealthtestctl.sh listtest` command. For example, to get the description of the test `SampleTest`, along with its parameters, use the following command:

```
./dfwhealthtestctl.sh descstest testname="SampleTest" showparam=Y
```

13.5.8 Listing Health Test Framework Test Runs

You can query the results of test runs, by test name, run name, status, or time, using the `dfwhealthtestctl.sh listrun` command:

- To query the results for a test run by specifying the test name:

```
./dfwhealthtestctl.sh listrun testname="SampleTest"
```
- To query the results for a test run by specifying the run name:

```
./dfwhealthtestctl.sh listrun runname="run_1"
```
- To query the results for a test run by specifying the status. For example, to get the results of all tests with a status of running:

```
./dfwhealthtestctl.sh listrun status=r
```
- To query the results for test runs that were started in the last 2 hours:

```
./dfwhealthtestctl.sh listrun lasthours=2
```

13.5.9 Generating Health Test Framework Reports

You can generate reports of the test runs for the Health Test Framework using the `dfwhealthtestctl.sh report` command. You can generate HTML or XML reports.

You can specify the run name, run ID or execution ID>

For example, to generate a report in HTML format for the run with the run ID of 1330128064268:

```
dfwhealthtestctl.sh report runid=1330128064268 format=HTML
```


Part VI

Advanced Administration

This part describes advanced administration tasks, such as managing the metadata repository and changing the network configuration, that involve reconfiguring Oracle Fusion Middleware.

Part VI contains the following chapters:

- [Chapter 14, "Managing the Metadata Repository"](#)
- [Chapter 15, "Changing Network Configurations"](#)

Managing the Metadata Repository

Many Oracle Fusion Middleware components use metadata repositories to hold configuration information about the component and metadata for applications. This chapter provides information on managing the metadata repositories used by Oracle Fusion Middleware.

It contains the following sections:

- [Section 14.1, "Understanding a Metadata Repository"](#)
- [Section 14.2, "Creating a Database-Based Metadata Repository"](#)
- [Section 14.3, "Managing the MDS Repository"](#)
- [Section 14.4, "Managing Metadata Repository Schemas"](#)
- [Section 14.5, "Purging Data"](#)

14.1 Understanding a Metadata Repository

A metadata repository contains metadata for Oracle Fusion Middleware components, such as Oracle Application Development Framework. It can also contain metadata about the configuration of Oracle Fusion Middleware and metadata for your applications.

Oracle Fusion Middleware supports multiple repository types. A repository type represents a specific schema or set of schemas that belong to a specific Oracle Fusion Middleware component (for example, Oracle Application Development Framework.) Oracle Fusion Middleware supports Edition-Based Redefinition (EBR), which enables you to upgrade the database component of an application while it is in use, thereby minimizing or eliminating down time. The schemas in a repository can be EBR-enabled schemas.

A particular type of repository, the Oracle Metadata Services (MDS) Repository, contains metadata for certain types of deployed applications. This includes custom Java EE applications developed by your organization and some Oracle Fusion Middleware component applications. For information related specifically to the MDS Repository type, see [Section 14.3](#).

You can create a database-based repository or, for MDS, a database-based repository or a file-based repository. For production environments, you use a database-based repository. Some components require that a schema be installed in a database, necessitating the use of a database-based repository. MDS supports Edition-Based Redefinition (EBR) enabled schemas.

Note: After the database for the metadata repository has been used for the Oracle Fusion Middleware installation, the database, service name, or SID cannot be changed.

14.2 Creating a Database-Based Metadata Repository

You use the Oracle Fusion Middleware Repository Creation Utility (RCU) to create the metadata repository in an existing database. You can use RCU to create the MDS Repository or a repository for metadata for particular components. RCU creates the necessary schemas for the components. See *Creating Schemas with the Repository Creation Utility* for a list of the schemas and their tablespaces and datafiles.

With RCU, you can also drop component schemas.

For information about the supported databases and the supported versions, as well as using these databases with the MDS Repository, see "Supported Databases for the MDS Schema" in the *Oracle Fusion Middleware System Requirements and Specifications*.

Note: Oracle recommends that all metadata repositories reside on a database at the same site as the components to minimize network latency issues.

For information about managing an MDS Repository, see [Section 14.3](#).

See Also: *Creating Schemas with the Repository Creation Utility* for information about how to use RCU to create a database-based metadata repository

14.3 Managing the MDS Repository

Oracle Metadata Services (MDS) Repository contains metadata for certain types of deployed applications. Those deployed applications can be custom Java EE applications developed by your organization and some Oracle Fusion Middleware component applications, such as Oracle B2B and Oracle Web Services Manager. A Metadata Archive (MAR), a compressed archive of selected metadata, is used to deploy metadata content to the MDS Repository, which contains the metadata for the application.

You should deploy your applications to MDS in the following situations, so that the metadata can be managed after deployment:

- The application contains seeded metadata packaged in a MAR.
- You want to enable user personalizations at run time.
- You have a SOA composite application (SCA).

The following topics provide information about the MDS Repository:

- [Understanding the MDS Repository](#)
- [Registering and Deregistering a Database-Based MDS Repository](#)
- [Registering and Deregistering a File-Based MDS Repository](#)
- [Changing the System Data Source](#)
- [Using System MBeans to Manage an MDS Repository](#)

- [Viewing Information About an MDS Repository](#)
- [Configuring an Application to Use a Different MDS Repository or Partition](#)
- [Moving Metadata from a Source System to a Target System](#)
- [Moving from a File-Based Repository to a Database-Based Repository](#)
- [Deleting a Metadata Partition from a Repository](#)
- [Purging Metadata Version History](#)
- [Managing Metadata Labels in the MDS Repository](#)

See Also: *High Availability Guide* for information about using an MDS Repository with Oracle Real Application Clusters (Oracle RAC)

14.3.1 Understanding the MDS Repository

The MDS framework allows you to create customizable applications. A customized application contains a base application (the base documents) and one or more layers containing customizations. MDS stores the customizations in a metadata repository and retrieves them at run time to merge the customizations with the base metadata to reveal the customized application. Since the customizations are saved separately from the base, the customizations are upgrade safe; a new patch to the base can be applied without breaking customizations. When a customized application is launched, the customization content is applied over the base application.

A customizable application can have multiple customization layers. Examples of customization layers are *industry* and *site*. Each layer can have multiple customization layer values, but typically only one such layer value from each layer is applied at run time. For example, the industry layer for a customizable application can contain values for health care and financial industries; but in the deployed customized application, only one of the values from this layer is used at a time. For more information about base documents and customization layers, see "Customizing Applications with MDS" in *Developing Fusion Web Applications with Oracle Application Development Framework*.

An MDS Repository can be file-based or database-based. For production environments, you use a database-based repository. You can have more than one MDS Repository for a domain.

A database-based MDS Repository provides the following features that are not supported by a file-based MDS Repository:

- **Efficient query capability:** A database-based MDS Repository is optimized for set-based queries. As a result, it provides better performance on such searches with the database repository.

The MDS Repository query API provides constructs to define the query operation and to specify conditions on metadata objects. These conditions are a set of criteria that restrict the search results to a certain set of attribute types and values, component types, text content, and metadata paths. The API allows multiple conditions to be combined to achieve dynamic recursive composition using OR and AND constructs.

- **Atomic transaction semantics:** A database-based MDS Repository uses the database transaction semantics, which provides rollbacks of failed transactions, such as failed imports or deployments.
- **Versioning:** A database-based MDS Repository maintains versions of the documents in a database-based repository. Versioning allows changes to metadata objects to be stored as separate versions rather than simply overwriting the

existing data in the metadata repository. It provides version history, as well as the ability to label versions so that you can access the set of metadata as it was at a given point in time.

- Isolate metadata changes: A database-based MDS Repository has the capability to isolate metadata changes in a running environment and test them for a subset of users before committing them for all users.
- Support for external change detection based on polling: This allows one application to detect changes that another application makes to shared metadata. For example, if you have an application deployed to Managed Servers A and B in a cluster, and you modify the customizations for the application deployed to Managed Server A, the data is written to the database-based repository. The application deployed to Managed Server B uses the updated customizations. This supports high availability (in particular, active/active scenarios.)
- Clustered updates: A database-based MDS Repository allows updates from multiple hosts to the metadata. For a file-based MDS Repository, updates can be made from only one host at a time.

Multiple applications can share metadata by configuring a shared metadata repository. When you do this, changes made by one application to the metadata in this repository are seen by other applications using the shared repository, if you configure external change detection for the applications.

In an MDS Repository, each application, including Oracle Fusion Middleware components, is deployed to its own partition. A **partition** is an independent logical repository within one physical MDS Repository, whether it is database-based or file-based.

For information about deploying applications and associating them with an MDS Repository, see [Chapter 10](#).

Note the following points about patching the MDS Repository:

- An MDS Repository must be registered with a domain before it is patched. Otherwise, the applied patches cannot be rolled back and no additional patches can be applied.
- You can apply patches to the following:
 - The MDS metadata
 - An MDS jar file
 - An MDS shared library
 - An MDS schema in the database-based metadata repository. The patch can include additive changes such as adding a new column or increasing the size of a column. Note that you cannot rollback this type of patch.
 - The MDS database PL/SQL in the database-based metadata repository. The patch can include changes to a PL/SQL package or new PL/SQL packages and procedures.
 - An MDS schema or PL/SQL in the database-based metadata repository that requires a corresponding MDS JAR file patch.

14.3.1.1 Databases Supported by MDS

The MDS Repository supports Oracle databases, as well as non-Oracle databases, including SQL Server, DB2, and MySQL.

For information about the supported databases and the supported versions, as well as using these databases with the MDS Repository, see "Supported Databases for the MDS Schema" in the *Oracle Fusion Middleware System Requirements and Specifications*.

14.3.1.2 Understanding MDS Operations

You can use Fusion Middleware Control or WLST commands to perform most operations on the MDS Repository. However, for some operations that do not have a custom user interface in Fusion Middleware Control or do not have WLST commands, you must use the System MBeans.

The sections that follow describe using Fusion Middleware Control and WLST commands to perform the operations, unless only System MBeans are supported. In that case, the sections describe how to use System MBeans to perform the operation.

You can view information about the repositories, including the partitions and the applications deployed to each partition. You can also perform operations on the partitions, such as purging, deleting, importing metadata, or exporting metadata.

Note the following when you use the MDS operations described in the sections that follow:

- The export operation exports a versioned stripe (either the tip version or based on a label) of metadata documents from an MDS Repository partition to a file system directory or archive. If you export to a directory, the directory must be accessible from the host where the application is running. If you export to an archive, the archive can be located on the system on which you are executing the command.

Because versioning of metadata is not supported for file-based repositories, the tip version (which is also the only version) is exported from a file-based repository.

- The import operation imports metadata documents from a file system directory or archive to an MDS Repository partition. If you exported to a directory, the directory must be accessible from the host where the application is running. If you exported to an archive, the archive can be located on the system on which you are executing the command.

If the target repository is a database-based repository, the metadata documents are imported as new tip versions. If the target repository is a file-based repository, the metadata documents are overwritten.

Note:

- To use the custom WLST MDS commands, you must invoke the WLST script from the Oracle Common home. See [Section 2.4.2](#) for more information.
 - For more information about the custom WLST MDS commands, see "Metadata Services (MDS) Custom WLST Commands" in the *WLST Command Reference for Infrastructure Components*.
-
-

[Table 14–1](#) lists the logical roles needed for each operation. The roles apply whether the operations are performed through the WLST commands, Fusion Middleware Control, or MBeans.

Table 14–1 MDS Operations and Required Roles

Operation	Logical Role
Clear cache	Operator role for application

Table 14–1 (Cont.) MDS Operations and Required Roles

Operation	Logical Role
Clone metadata partition	Admin role for domain
Create metadata label	Admin role for application
Create metadata partition	Admin role for domain
Delete metadata	Admin role for application
Delete metadata label	Admin role for application
Delete metadata partition	Admin role for domain
Deregister metadata database repository	Admin role for domain
Deregister metadata file repository	Admin role for domain
Destroy sandbox	Admin role for application
Export metadata	Monitor role for application
Export sandbox metadata	Monitor role for application
Import MAR	Admin role for application
Import metadata	Admin role for application
Import sandbox metadata	Admin role for application
List metadata label	Monitor role for application
List sandboxes	Monitor role for application
Promote metadata label	Admin role for application
Purge metadata	Admin role for application
Purge metadata labels	Admin role for application
Register metadata database repository	Admin role for domain
Register metadata file repository	Admin role for domain

For information about how these roles map to WebLogic Server roles, see "Mapping of Logical Roles to WebLogic Roles" in *Securing Applications with Oracle Platform Security Services*.

14.3.2 Registering and Deregistering a Database-Based MDS Repository

The following topics describe how to register and deregister a database-based MDS Repository:

- [Registering a Database-Based MDS Repository Using Fusion Middleware Control](#)
- [Deregistering a Database-Based MDS Repository](#)

Note: Note the following if you invoke the following WLST commands or comparable MBeans in a script:

- registerMetadataDBRepository
- deregisterMetadataDBRepository

In this release and previous releases, the commands or MBeans have the following behavior:

1. Starts an Oracle WebLogic Server editing session.
2. Registers or deregisters the repository.
3. Activates the changes.

However, you can start an editing session explicitly. If you do, the automatic activation of the changes are deprecated.

14.3.2.1 Registering a Database-Based MDS Repository

Before you can deploy an application to an MDS Repository, you must register the repository with the Oracle WebLogic Server domain. You can register a database-based MDS Repository using Fusion Middleware Control or WLST, as described in the following topics:

- [Registering a Database-Based MDS Repository Using Fusion Middleware Control](#)
- [Registering a Database-Based MDS Repository Using WLST](#)

14.3.2.1.1 Registering a Database-Based MDS Repository Using Fusion Middleware Control

You create a database-based MDS Repository using RCU, as described in [Section 14.2](#).

To register a database-based MDS Repository using Fusion Middleware Control:

1. From the WebLogic Domain menu, choose **Other Services**, then **Metadata Repositories**.

The Metadata Repositories page is displayed, as shown in the following figure:

Metadata Repositories

You create most Fusion Middleware component schema repositories in a database using the Repository Creation Utility. Metadata Services (MDS) repositories can be created in a database with the Repository Creation Utility or created on disk as file-based repositories. You must register an MDS repository before you can deploy application metadata to the repository.

Database-Based Repositories

Register...		Deregister...	
Repository Name	Database Type	Database Name	Schema Name
mds-soa	Oracle	ORCL.US.ORACLE.COM	DEV59_M
mds-owsm	Oracle	ORCL.US.ORACLE.COM	DEV59_M
mds-bam	Oracle	ORCL.US.ORACLE.COM	DEV59_M

File-Based Repositories

Register...		Deregister...	
Repository Name	Directory		
No Repository			

2. In the Database-Based Repositories section, click **Register**.
The Register Database-Based Metadata Repository page is displayed.
3. In the Database Connection section, enter the following information:
 - For **Database Type**, select the type of database.
 - For **Host Name**, enter the name of the host.
 - For **Port**, enter the port number for the database, for example: 1521.
 - For **Service Name**, enter the service name for the database. The default service name for a database is the global database name, comprising the database name, such as `orcl`, and the domain name. In this case, the service name would be `orcl.domain_name.com`.
 - For **User Name**, enter a user name for the database which is assigned the SYSDBA role, for example: `SYS`.
 - For **Password**, enter the password for the user.
 - For **Role**, select a database role, for example, **SYSDBA**.
4. Click **Query**.

A table is displayed that the metadata repositories in the database, as shown in the following figure:

soa_domain ⓘ Logged in as **weblogic**
WebLogic Domain ▾ Page Refreshed Mar 20, 2014 12:04:39 PM PDT ↻

Register Database-Based Metadata Repository ?

A repository stores information used by Application Server components and other applications. A metadata repository must be registered to be operational. A database-based repository is created using the Repository Creation Utility. To register, input database connection information and click Query, then select one of the Metadata Repository and click OK button.

Database Connection Information

Database Type: Oracle SQL Server IBM DB2 MySQL

* User Name: * Password: Role:

* Host Name:

* Port:

* Service Name:

Metadata Repository	Is Registered?	Schema Name	Version	Status
MDS	false	DEV37_MDS	11.1.1.7.0	VALID
MDS	false	SOAEDG70_MDS	12.1.3.0.0	VALID
MDS	false	LJ1212_MDS	12.1.2.0.0	VALID
MDS	false	DEV2_MDS	12.1.2.0.0	VALID
MDS	false	DEV3_MDS	12.1.2.0.0	VALID

5. Select a repository, then enter the following information:

- For **Repository Name**, enter a name.
- For **Schema Password**, enter the password you specified when you created the schema.

6. Click **OK**.

The repository is registered with the Oracle WebLogic Server domain and is targeted to the Administration Server. To target the repository to other servers, see [Section 14.3.2.2](#).

In addition, a system data source is created with the name *mds-repository_name*. Global transaction support is disabled for the data source.

14.3.2.1.2 Registering a Database-Based MDS Repository Using WLST To register a database-based MDS Repository using the command line, you use the WLST `registerMetadataDBRepository` command. For example, to register the MDS Repository `mds-repos1`, use the following command:

```
registerMetadataDBRepository(name='mds-repos1', dbVendor='ORACLE',
    host='hostname', port='1521', dbName='ora11',
    user='username', password='password', targetServers='server1')
```

14.3.2.2 Adding or Removing Servers Targeted to the MDS Repository

When you register an MDS Repository using Fusion Middleware Control, the repository is targeted to the Administration Server. You can target the repository to additional servers or remove servers as targets.

To target the MDS Repository to additional servers:

1. From the navigation pane, expand **Metadata Repositories**.
2. Select the repository.

The repository home page is displayed, as shown in the following figure:

The screenshot shows the Oracle MDS Repository Administration console for the repository 'mds-test_repo'. The user is logged in as 'weblogic'. The page was refreshed on Mar 20, 2014 at 12:11:55 PM PDT.

Repository Partitions

To select a partition click on a row in the Repository Partitions table.

Buttons: Delete ... Manage Labels

Repository Partition	Applications	Read			V
		Response (seconds)	Load (reads/second)	Response (seconds)	
essapp-internal-partition	🔗	0	0	0	▲
ess-partition	🔗	0	0	0	☰
essUserMetadata	🔗	0	0	0	▼
owsm	🔗	0	0	0	

Targeted Servers

The repository is accessible from the servers listed below:

Buttons: + Add ... - Remove ...

Server: AdminServer

Read Response and Load

Graph showing Document read time (in seconds) and Number of documents read per second.

X-axis: 11:58 AM, 12:02 PM, 12:06, 12:10, March 20 2014

Legend: Document read time (in seconds) (blue square), Number of documents read per second (red square)

Table View

Resource Center

3. In the Targeted Servers section, click **Add**.
The Target the Repository dialog box is displayed.
 4. Select the server or cluster and click **Target**.
You can expand the cluster to see the servers in the cluster. However, if you select a cluster, the repository is targeted to all servers in the cluster.
 5. When the operation completes, click **Close**.
The server is now listed in the Targeted Servers section.
- To remove a server as a target for the repository:
1. From the navigation pane, expand **Metadata Repositories**.
 2. Select the repository.
The repository home page is displayed.
 3. In the Targeted Servers section, select the target server and click **Remove**.
The Untarget the Repository dialog box is displayed.
 4. Select the server or cluster and click **Untarget**.
You can expand the cluster to see the servers in the cluster. However, if you select a cluster, the repository will be untargeted from all servers in the cluster.
 5. When the operation completes, click **Close**.

14.3.2.3 Deregistering a Database-Based MDS Repository

Deregistration does not result in loss of data stored in the repository. However, any applications using a deregistered repository will not function after the repository is deregistered. You must ensure that no application is using the repository before you deregister it.

You can deregister a database-based MDS Repository using Fusion Middleware Control or WLST, as described in the following topics:

- [Deregistering a Database-Based MDS Repository Using Fusion Middleware Control](#)
- [Deregistering a Database-Based MDS Repository Using WLST](#)

14.3.2.3.1 Deregistering a Database-Based MDS Repository Using Fusion Middleware Control

To deregister an MDS Repository using Fusion Middleware Control:

1. From the WebLogic Domain menu, choose **Other Services**, then **Metadata Repositories**.

The Metadata Repositories page is displayed.

Alternatively, you can navigate to the Register Metadata Repositories page by choosing **Administration**, then **Register/Deregister** from the Metadata Repository menu when you are viewing a metadata repository home page.

2. Select the repository from the table.
3. Click **Deregister**.
4. Click **Yes** in the Confirmation dialog box.

14.3.2.3.2 Deregistering a Database-Based MDS Repository Using WLST To deregister a database-based MDS Repository using the command line, you use the WLST `deregisterMetadataDBRepository` command. For example, to deregister the MDS Repository `mds-repos1`, use the following command:

```
deregisterMetadataDBRepository(name='mds-repos1')
```

14.3.3 Registering and Deregistering a File-Based MDS Repository

The following topics describe how to create, register, and deregister a file-based metadata repository:

- [Creating and Registering a File-Based MDS Repository](#)
- [Deregistering a File-Based MDS Repository](#)

Note: Note the following if you invoke the following MBeans in a script:

- registerMetadataFileRepository
- deregisterMetadataFileRepository

In this release and previous releases, the MBeans have the following behavior:

1. Starts an Oracle WebLogic Server editing session.
2. Registers or deregisters the repository.
3. Activates the changes.

However, you can start an editing session explicitly. If you do, the automatic activation of the changes are deprecated.

14.3.3.1 Creating and Registering a File-Based MDS Repository

You can create a file-based MDS Repository and register it with an Oracle WebLogic Server domain using Fusion Middleware Control.

To create and register a file-based repository using Fusion Middleware Control:

1. From the WebLogic Domain menu, choose **Other Services**, then **Metadata Repositories**.

The Metadata Repositories page is displayed.

2. In the File-Based Repository section, click **Register**.

The Register Metadata Repository page is displayed.

3. Enter the following information:

- For **Name**, enter a name. For example, enter repos1. The prefix `mds-` is added to the name and a repository with the name `mds-repos1` is registered. If you enter a name that begins with `mds-`, a repository with the given name is registered.
- For **Directory**, specify the directory. The Administration Server and Managed Servers that run the applications that use this repository must have write access to the directory.

Note the following:

- If the specified path exists on the file system, the metadata file repository is registered; all the subdirectories under this path are automatically loaded as partitions of this file-based repository.
- If the path specified does not exist, a directory with this name is created on the file system during the registration. Because there are no partitions created yet, there are no subdirectories to load.
- If the specified path is invalid and cannot be created for some reason, such as permission denied, an error is displayed and the registration fails.
- If the specified path exists, but as a file not a directory, an error is not displayed and the registration succeeds.

4. Click **OK**.

The repository is created and registered and is displayed on the Metadata Repositories page.

You can now create and delete partitions. Those changes are reflected in the directory on the file system.

You can also create a file-based repository using system MBeans. For information about using the System MBean Browser, see [Section 14.3.5](#).

14.3.3.2 Deregistering a File-Based MDS Repository

You can deregister a file-based MDS Repository using Fusion Middleware Control.

To deregister a file-based repository using Fusion Middleware Control:

1. From the WebLogic Domain menu, choose **Other Services**, then **Metadata Repositories**.

The Metadata Repositories page is displayed.

2. In the File-Based Repository section, select the repository and click **Deregister**.
3. Click **OK** in the Confirmation dialog box.

If the file-based repository is valid, it is removed from the repository list. Otherwise, an error is displayed.

You can also deregister a file-based repository using system MBeans. For information about using the System MBean Browser, see [Section 14.3.5](#).

14.3.4 Changing the System Data Source

You can change the system data source to reassociate an application to a new repository. You can change the database or the schema that contains the data source. To do so, you can use Oracle WebLogic Server Administration Console or Fusion Middleware Control. To use Fusion Middleware Control:

1. From the WebLogic Domain menu, choose **JDBC Data Sources**.

The JDBC Data Sources page is displayed.

2. Select the data source you want to change.

The JDBC Data Source page for the selected data source is displayed.

3. Select the Connection Pool tab.
4. To change the database, modify the **Database URL** field. For example:

```
jdbc:oracle:thin:@hostname.domainname.com:1522/orcl
```

5. For **Password**, enter the password for the database.
6. To change the schema, modify the Properties section, changing the value for **user**.
7. If the database is a DB2 database, add the property `sendStreamAsBlob`, with a value of `true`.
8. Click **Apply**.
9. Restart the servers that use this data source.

14.3.5 Using System MBeans to Manage an MDS Repository

Although most procedures in this chapter discuss using Fusion Middleware Control or WLST to manage the MDS Repository, you can also use system MBeans:

1. From the WebLogic Domain menu, choose **System MBean Browser**.

The System MBean Browser page is displayed.

2. In the page's navigation pane, expand **Application Defined MBeans**, then expand **oracle.mds.lcm**. Expand the domain, then **MDSDomainRuntime**, and then select **MDSDomainRuntime**.
3. In the Application Defined MBeans pane, select the Operations tab.
4. Click one of the operations, such as **registerMetadataFileRepository**.

The Operations page is displayed.

5. In the Value column, enter values for the operation.
6. Click **Invoke**.

14.3.6 Viewing Information About an MDS Repository

You can view information about an MDS Repository using Fusion Middleware Control or system MBeans, as described in the following topics:

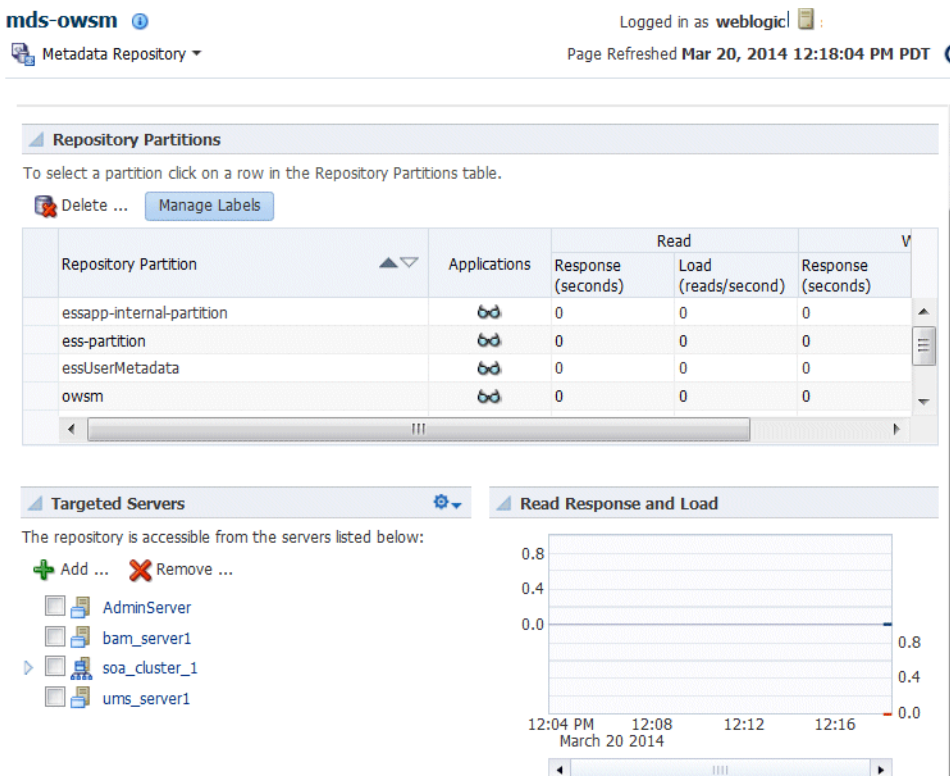
- [Viewing Information About an MDS Repository Using Fusion Middleware Control](#)
- [Viewing Information About an MDS Repository Using System MBeans](#)

14.3.6.1 Viewing Information About an MDS Repository Using Fusion Middleware Control

To view information about an MDS Repository using Fusion Middleware Control:

1. From the navigation pane, expand **Metadata Repositories**.
2. Select the repository.

The following figure shows the home page for an MDS Repository:



3. To see which applications use the repository, click the icon in the Applications column. The Applications using the partition dialog box is displayed, with tabs for Deployed Applications and Referenced by Applications:
 - The Deployed Applications tab shows the list of applications whose metadata is deployed to the repository partition.
 - The Referenced by Applications tab shows the list of applications that refer to the metadata stored in the repository partition.

From this page, you can also:

- Delete partitions, as described in [Section 14.3.10.1](#).
- Delete labels, as described in [Section 14.3.12.5](#).
- Add or remove targeted servers, as described in [Section 14.3.2.2](#).

14.3.6.2 Viewing Information About an MDS Repository Using System MBeans

You can use the System MBean operations `listPartitions`, `listRepositories`, and `listRepositoryDetails` to get a list of partitions in the repository, a list of repositories, and details of the repository registered with the domain:

1. From the WebLogic Domain menu, choose **System MBean Browser**.
The System MBean Browser page is displayed.
2. In the page's navigation pane, expand **Application Defined MBeans**, then expand **oracle.mds.lcm**. Expand the domain, then **MDSDomainRuntime**, and then select **MDSDomainRuntime**.
3. In the Application Defined MBeans pane, select the Operations tab.
4. Click one of the operations, such as `listPartitions`, `listRepositories`, and `listRepositoryDetails`.
The Operations page is displayed.
5. Click **Invoke**.
The information is displayed in the Return Value table.

For information about changing the MDS configuration attributes for an application, see [Section 10.8](#).

14.3.7 Configuring an Application to Use a Different MDS Repository or Partition

When you deploy an application, you can associate it with an MDS Repository. You can subsequently change the MDS Repository or partition to which an application is associated, using WLST or Fusion Middleware Control. For example, a different repository contains different metadata that needs to be used for a particular application.

To associate an application with a new MDS Repository or partition, you can either:

- Redeploy the application, specifying the new repository or partition.
To create a new partition, you can either:
 - Clone the partition to a different repository. Cloning the partition is valid only with a database-based repository with databases of the same type and version. When you clone the partition, you preserve the metadata version history, including any customizations and labels.

[Section 14.3.7.1](#) describes how to clone a partition and how to redeploy the application, specifying the partition that you have cloned.

- Create a new partition, then export the metadata from the current partition and import the metadata into the new partition.

[Section 14.3.7.2](#) describes how to create the partition and export and import data and how to redeploy the application, specifying the new repository or partition.

- Change the system data source. When you change the system data source, you can change the database or the schema in which it is stored.

[Section 14.3.4](#) describes how to change the system data source.

14.3.7.1 Cloning a Partition

You can clone a partition to the same repository or a different repository using the system MBean `cloneMetadataPartition`. Both the original repository and the target repository must be a database-based repository.

To clone the partition, and then redeploy the application to a new repository or to the same repository:

1. Clone the partition, using the `cloneMetadataPartition` operation on the system MBean. The following example clones `partition1` from the old repository to the new repository:
 - a. In Fusion Middleware Control, from the navigation pane, navigate to the Managed Server from which the application is deployed. From the WebLogic Server menu, choose **System MBean Browser**.
The System MBean Browser page is displayed.
 - b. In the System MBean Browser's navigation pane, expand **Application Defined MBeans**, then expand **oracle.mds.lcm**. Expand the domain, and then **MDSDomainRuntime**. Select **MDSDomainRuntime**.
 - c. In the Application Defined MBeans pane, select the Operations tab.
The following figure shows the System MBeans Browser with the Application Defined MBeans pane:

soa_server1 ⓘ 📄 WebLogic Server 🟢 Start Up 🔴 Shut Down... 👤 Logged in as weblogic 🔄 Page Refreshed Mar 20, 2014 12:20:40 PM PDT

/Domain_soa_domain/soa_domain/soa_server1 > System MBean Browser

System MBean Browser

- oracle.as.soainfra.config
- oracle.as.util
- oracle.beam.server
- oracle.dfw
- oracle.dms
- oracle.dms.context
- oracle.dms.event.config
- oracle.dms.instrument
- oracle.em.cw
- oracle.j2ee.config
- oracle.jrf
- oracle.jrf.server
- oracle.logging
- oracle.mds.lcm
 - Domain: soa_domain
 - MDSDomainRuntime
 - MDSDomainRuntime**
 - Server: AdminServer
 - Server: soa_server1

Application Defined MBeans: MDSDomainRuntime:MDSI...

Show MBean Information

Attributes **Operations** Notifications

Name	Description
1 cloneMetadataPartition	Clones the given repository partition.
2 createMetadataPartition	Creates a new metadata partition in the specified repository.
3 deleteMetadataLabels	Delete metadata labels
4 deleteMetadataLabels	Delete metadata labels
5 deleteMetadataPartition	Deletes the specified repository partition and all the documents within the partition.
6 deprovisionTenant	Deprovision a tenant
7 deregisterMetadataDBRepository	Deregisters DB metadata repository from the Domain.
8 deregisterMetadataFileRepository	Deregisters File metadata repository from the Domain.
9 isRepositoryTargeted	Is the repository targeted on server or cluster?
10 listMetadataLabels	List metadata labels
11 listMetadataLabels	List metadata labels
12 listPartitions	Lists all metadata partitions in the repository.

d. Select **cloneMetadataPartition**.

The Operation: cloneMetadataPartition page is displayed.

e. In the Parameters table, enter the following values:

- For **fromRepository**, enter the name of the metadata repository that contains the metadata partition from which the metadata documents are to be cloned.
- For **fromPartition**, enter the name of the partition from which the metadata documents are to be cloned.
- For **toRepository**, enter the name of the metadata repository to which the metadata documents from the source repository partition are to be cloned.
- For **toPartition**, enter the name of metadata repository partition to be used for the target partition. The name must be unique within the repository. If you do not supply a value for this parameter, the name of the source partition is used for the target partition.

If the toRepository name is the same as the original repository, you must enter a partition name and the name must be unique within the repository.

f. Click **Invoke**.

g. Verify that the partition has been created by selecting the repository in the navigation pane. The partition is listed in the Partitions table on the Metadata Repository home page.

2. Redeploy the application, as described in [Section 10.4.3](#) or [Section 10.5.3](#), depending on the type of application. When you do so, you specify the new partition and repository in the Application Attributes page:

- To change the repository, click the icon next to the **Repository Name**. In the Metadata Repositories dialog box, select the repository and click **OK**.
- To change the partition, enter the partition name in **Partition Name**.

14.3.7.2 Creating a New Partition and Reassociating the Application to It

You can create a new partition in the same or a different repository by redeploying the application and specifying the new partition. Then, you transfer the metadata to the new partition using WLST.

You can use this procedure to transfer metadata between two different types of repositories (file-based to database-based or from an Oracle Database to another database.)

To create a new partition and reassociate the application to it:

1. Export the metadata from the source partition to a directory on the file system using the WLST `exportMetadata` command:

```
exportMetadata(application='sampleApp', server='server1',
               toLocation='/tmp/myrepos/mypartition', docs='/**')
```

2. Redeploy the application, as described in [Section 10.4.3](#) or [Section 10.5.3](#), depending on the type of application. When you do so, you specify the new partition and repository in the Application Attributes page:
 - a. To change the repository, click the icon next to the **Repository Name**. In the Metadata Repositories dialog box, select the repository and click **OK**.
 - b. To change the partition, enter the partition name in **Partition Name**.
3. Import the metadata from the file system to the new partition using the WLST `importMetadata` command:

```
importMetadata(application='sampleApp', server='server1',
               fromLocation='/tmp/myrepos/mypartiton', docs='/**')
```

4. Optionally, deregister the original repository, as described in [Section 14.3.3.2](#) or [Section 14.3.2.3](#).

Alternatively, you can create a new partition using the WLST command `createMetadataPartition`. The partition name must be unique within the repository. If the partition parameter is missing, the name of the source partition is used for the target partition. The following example creates the partition `partition1`:

```
createMetadataPartition(repository='mds-repos1', partition='partition1')
```

14.3.8 Moving Metadata from a Source System to a Target System

You can transfer the metadata in MDS from one partition to another. As an example, you want to move an application from a test system to a production system. You have a test application that is deployed in a domain in the test system and a production application deployed in a domain in the production system. You want to transfer the customizations from the test system to the production system. To do that, you transfer the metadata from the partition in the test system to a partition in the production system.

To transfer the metadata from one partition to another, you export the metadata from the partition and then import it into the other partition. You can use Fusion Middleware Control or WLST to transfer the metadata, as described in the following topics:

- [Transferring Metadata Using Fusion Middleware Control](#)
- [Transferring Metadata using WLST](#)

14.3.8.1 Transferring Metadata Using Fusion Middleware Control

To use Fusion Middleware Control to transfer metadata:

1. From the navigation pane, expand **Application Deployments**, then select the application.
2. From the Application Deployment menu, choose **MDS Configuration**.

The MDS Configuration page is displayed, as shown in the following figure:

The screenshot shows the MDS Configuration page for the application 'mdsappdb1'. The page is titled 'MDS Configuration' and shows the 'Target Metadata Repository' section with the following details:

Repository	mds-soa
Type	Database
Partition	partition1

Below the table, there are two main sections: 'Export' and 'Import'.

Export Section:

- Export a versioned stripe of metadata documents from a metadata repository partition to a file system directory or archive. Only the tip version will be exported for a file repository.
- Export metadata documents to an archive on the machine where this web browser is running.
- Export metadata documents to a directory or archive on the machine where this application is running.
- Exclude base documents

Import Section:

- Import metadata documents from a file system directory or archive to a metadata repository partition. If the target metadata repository is a database repository, the documents will be imported as new tip versions.
- Import metadata documents from an archive on the machine where this web browser is running.
- Import metadata documents from a directory or archive on the machine where this application is running.

3. In the Export section, select one of the following:

- **Export metadata documents to an archive on the machine where this web browser is running.**

Click **Export**.

The export operation exports a zip file. Depending on the operating system and browser, a dialog box is displayed that asks you if you want to save or open the file.

- **Export metadata documents to a directory or archive on the machine where this application is running.**

Enter a directory location or archive to which the metadata can be exported.

The target directory or archive file (.jar, .JAR, .zip or .ZIP) to which to transfer the documents selected from the source partition. If you export to a directory, the directory must be a local or network directory or file where the application is physically deployed. If you export to an archive, the archive can be located on a local or network directory or file where the application is physically deployed, or on the system on which you are executing the command.

If the location does not exist in the file system, a directory is created except that when the names ends with .jar, .JAR, .zip or .ZIP, an archive file is created.

If the archive file already exists, the `exportMetadata` operation overwrites the file.

Click **Export**. Then, in the Confirmation dialog box, click **Close**.

If you check **Exclude base documents**, this operation exports only the customizations, not the base documents. See [Section 14.3.1](#) for information about base documents and customizations.

4. If the target application is on a different system, copy the exported metadata to that system.
5. From the navigation pane for the target system, expand **Application Deployments**, then select the application.
6. From the Application Deployment menu, choose **MDS Configuration**.
The MDS Configuration page is displayed
7. In the Import section, select one of the following:
 - **Import metadata documents from an archive on the machine where this web browser is running.**
 - **Import metadata documents from a directory or archive on the machine where this application is running.**

Enter the location of the directory or archive that contains the exported metadata. If you specify a directory, include the subdirectory with the partition name in the specification. The directory or archive file must be a local or network directory or file where the application is physically deployed.

8. Click **Import**.
9. In the Confirmation dialog box, click **Close**.

14.3.8.2 Transferring Metadata using WLST

To use WLST to transfer metadata:

1. Export the metadata from the original partition using the `exportMetadata` command:

```
exportMetadata(application='sampleApp', server='server1',
               toLocation='/tmp/myrepos/mypartition', docs='/**')
```

This command exports a versioned stripe of the metadata documents from the metadata partition to a file system directory. Only customization classes declared in the `cust-config` element of `adf-config.xml` are exported. If there is no `cust-config` element declared in `adf-config.xml`, all customization classes are exported.

To export all customizations, use the option `restrictCustTo=""`.

2. If the production application is on a different system, copy the exported metadata to that system.
3. Import the metadata to the other partition using the WLST `importMetadata` command:

```
importMetadata(application='sampleApp', server='server1',
               fromLocation='/tmp/myrepos/mypartiton', docs='/**')
```

The value of the `fromLocation` parameter must be on the same system that is running WLST or on a mapped network drive or directory mount. You cannot use direct network references such as `\\mymachine\repositories\`.

Only customization classes declared in the cust-config element of adf-config.xml are imported. If there is no cust-config element declared in adf-config.xml, all customization classes are imported.

To import all customizations, use the option restrictCustTo="%".

14.3.9 Moving from a File-Based Repository to a Database-Based Repository

You can move from a file-based repository to a database-based repository. (You cannot move from a database-based repository to a file-based repository.)

To minimize downtime, take the following steps to move an application's metadata from a file-based repository to a database-based repository:

1. Use RCU to create schemas in the new repository, as described in [Section 14.2](#).
2. Create a new partition using the WLST command `createMetadataPartition` with same name as source partition:

```
createMetadataPartition(repository='mds-repos1', partition='partition1')
```

3. Export the metadata from the source partition to a directory on the file system:

```
exportMetadata(application='sampleApp', server='server1',
               toLocation='/tmp/myrepos/partition1', docs='/**')
```

4. Import the metadata from the file system to the new partition:

```
importMetadata(application='sampleApp', server='server1',
               fromLocation='/tmp/myrepos/partition1', docs='/**')
```

5. Redeploy the application, as described in [Section 10.4.3](#) or [Section 10.5.3](#), depending on the type of application. When you do so, you specify the new partition and repository in the Application Attributes page:
 - a. To change the repository, click the icon next to the **Repository Name**. In the Metadata Repositories dialog box, select the repository and click **OK**.
 - b. To change the partition, enter the partition name in **Partition Name**.
6. Deregister the file-based repository, as described in [Section 14.3.3.2](#).

14.3.10 Deleting a Metadata Partition from a Repository

You can delete metadata partitions if there are no applications either deployed to the partition or referring to the partition. You may want to delete a metadata partition from the repository in the following circumstances:

- When you undeploy an application. Oracle Fusion Middleware leaves the metadata partition because you may still want the metadata, such as user customizations, in the partition. If you do not need the metadata, you can delete the partition.
- When you have transferred metadata from one partition to another and configured the application to use the new partition.
- When you have cloned a partition and configured the application to use the new partition.

Note that deleting a partition deletes all the data contained in the partition.

You can delete a metadata partition using WLST or Fusion Middleware Control, as described in the following topics:

- [Deleting a Metadata Partition Using Fusion Middleware Control](#)
- [Deleting a Metadata Partition Using WLST](#)

14.3.10.1 Deleting a Metadata Partition Using Fusion Middleware Control

To delete a metadata partition from a repository partition using Fusion Middleware Control:

1. From the navigation pane, expand **Metadata Repositories**.
2. Select the repository.
The repository home page is displayed.
3. In the Repository Partitions section, select the partition and click **Delete**.
4. In the confirmation dialog box, click **OK**.

14.3.10.2 Deleting a Metadata Partition Using WLST

To delete a metadata partition from a repository, you can use the WLST command `deleteMetadataPartition`. For example, to delete the metadata partition from the file-based repository `mds-repos1`, use the following command:

```
deleteMetadataPartition(repository='mds-repos1', partition='partition1')
```

14.3.11 Purging Metadata Version History

For database-based MDS Repositories, you can purge the metadata version history from a partition. (File-based MDS Repositories do not maintain version history.) This operation purges version history of unlabeled documents from the application's repository partition. The tip version (the latest version) is not purged, even if it is unlabeled.

To purge metadata labels, you use the `purgeMetadataLabels` command, as described in [Section 14.3.12.4](#). Then, you can purge the metadata version history.

Consider purging metadata version history on a regular basis as part of MDS Repository maintenance, when you suspect that the database is running out of space or performance is becoming slower. This operation may be performance intensive, so plan to do it in a maintenance window or when the system is not busy. Note that MDS purges 300 documents in each iteration, commits the change, and repeats until all purgeable documents are processed.

For specific recommendations for particular types of applications, see the documentation for a particular component.

You can purge metadata version history using WLST or Fusion Middleware Control, as described in the following topics:

- [Purging Metadata Version History Using Fusion Middleware Control](#)
- [Purging Metadata Version History Using WLST](#)
- [Enabling Auto-Purge](#)

14.3.11.1 Purging Metadata Version History Using Fusion Middleware Control

To use Fusion Middleware Control to purge the metadata version history:

1. From the navigation pane, expand **Application Deployments**, then select the application.
2. From the Application Deployment menu, choose **MDS Configuration**.

For Oracle SOA Suite, you can expand **SOA** in the navigation tree, then select **soa-infra**. From the SOA Infrastructure menu, select **Administration**, then **MDS Configuration**.

The MDS Configuration page is displayed.

3. In the Purge section, in the **Purge all unlabeled past versions older than** field, enter a number and select the unit of time. For example, enter **3** and select **months**.
4. Click **Purge**.
5. In the Confirmation dialog box, click **Close**.

14.3.11.2 Purging Metadata Version History Using WLST

To use WLST to purge metadata version history, use the `purgeMetadata` command. You specify the documents to be purged by using the `olderThan` parameter, specifying the number of seconds. The following example purges all documents older than 100 seconds:

```
purgeMetadata(application='sampleApp', server='server1', olderThan=100)
```

14.3.11.3 Enabling Auto-Purge

You can enable automatic purging using the MDSAppConfig MBean:

1. From the WebLogic Domain menu, choose **System MBean Browser**.
The System MBean Browser page is displayed.
2. Expand **Application Defined MBeans**, then **oracle.adf.share.config**, then **Server: name**, then **Application: name**, then **ADFConfig**, then **ADFConfig**, and **ADFConfig**.
3. Select **MDSAppConfig**.
The Application Defined MBeans page is displayed.
4. For **AutoPurgeTimeToLive**, enter a value, in seconds.
5. Navigate up to **ADFConfig** (the parent of **MDSAppConfig**) and select it.
6. In the Operations tab, click **Save**.

14.3.12 Managing Metadata Labels in the MDS Repository

A **metadata label** is a means of selecting a particular version of each object from a metadata repository partition. Conceptually, it is a collection of document versions, one version per document, representing a *horizontal stripe* through the various document versions. This stripe comprises the document versions which were the tip versions (latest versions) at the time the label was created.

You can use a label to view the metadata as it was at the point in time when the label was created. You can use the WLST commands to support logical backup and recovery of an application's metadata contained in the partition.

Labels are supported only in database-based repositories.

Document versions belonging to a label are not deleted by automatic purging, unless the label is explicitly deleted. In this way, creating a label guarantees that a view of the metadata as it was at the time the label was created remains available until the label is deleted.

When an application that contains a MAR is deployed, a label with the prefix `postDeployLabel_` is created. For example: `postDeployLabel_mdsappdb_mdsappdb.mar_2556916398`.

Each time you patch the MAR, a new deployment label is created, but the previous deployment label is not deleted. Similarly, when you undeploy an application that contains a MAR, the application is undeployed, but the label remains in the metadata repository partition.

If you delete a deployment label, when the application is restarted, the MAR is automatically redeployed, and the deployment label is also re-created.

The following topics describe how to manage labels:

- [Creating Metadata Labels](#)
- [Listing Metadata Labels](#)
- [Promoting Metadata Labels](#)
- [Purging Metadata Labels](#)
- [Deleting Metadata Labels](#)

14.3.12.1 Creating Metadata Labels

To create a label for a particular version of objects in a partition in an MDS Repository, you use the WLST command `createMetadataLabel`. For example, to create a label named `prod1` for the application `my_mds_app`, use the following command:

```
createMetadataLabel(application='my_mds_app', server='server1', name='prod1')
Executing operation: createMetadataLabel.
```

```
Created metadata label "prod1".
```

If the application has more than one version, you must use the `applicationVersion` parameter to specify the version.

14.3.12.2 Listing Metadata Labels

You can list the metadata labels for a particular application. To do so, use the WLST command `listMetadataLabel`. For example, to list the labels for the application `my_mds_app`, use the following command:

```
listMetadataLabels(application='my_mds_app', server='server1')
Executing operation: listMetadataLabels.
```

```
Database Repository partition contains the following labels:
```

```
prod1
prod2
postDeployLabel_mdsappdb_mdsappdb.mar_2556916398
```

If the application has more than one version, you must use the `applicationVersion` parameter to specify the version.

14.3.12.3 Promoting Metadata Labels

You can promote documents associated with a metadata label so that they become the latest version. That is, you can promote them to the tip. Promote a label if you want to roll back to an earlier version of all of the documents captured by the label.

To promote a label to the tip, use the WLST command `promoteMetadataLabel`. For example to promote the label `prod1`, use the following command:

```
promoteMetadataLabel(application='my_mds_app', server='server1', name='prod1')
Location changed to domainRuntime tree. This is a read-only tree with DomainMBean
as the root.
For more help, use help(domainRuntime)
```

Executing operation: promoteMetadataLabel.

Promoted metadata label "prod1" to tip.

If the application has more than one version, you must use the `applicationVersion` parameter to specify the version.

14.3.12.4 Purging Metadata Labels

You can purge metadata labels that match the given name pattern or age, allowing you to purge labels that are no longer in use. This reduces the size of the database, improving performance. You must delete the labels associated with unused metadata documents before you can purge the documents and revision history from the repository.

You may want to delete a label for older applications that were undeployed, but the labels were not deleted. Each time you patch the MAR, a new label is created, but the previous label is not deleted.

You can use Fusion Middleware Control or WLST to purge metadata labels, as described in the following topics:

- [Purging Metadata Labels Using Fusion Middleware Control](#)
- [Purging Metadata Labels Using WLST](#)

14.3.12.4.1 Purging Metadata Labels Using Fusion Middleware Control To purge metadata labels using Fusion Middleware Control:

1. Expand **Metadata Repositories**.
2. Select the repository.
The repository home page is displayed.
3. Select a partition and click **Manage Labels**.

The Manage Labels page is displayed, as shown in the following figure:

Repository Partition: owsm

Use this page to find and delete metadata labels that are no longer in use within the selected partition.

By default, the table lists all the metadata labels created more than one year ago. To show newer labels in the partition, specify the label search criteria and press Search.

For more information, click the online help icon at the top of the page.

Search Labels

* Required

Match All Any

* Label Name Like %

* Age Older Than 1

* Age (units) Equals Years

Search Reset

Delete?	Name	Description	Age	Creation Time
No labels found.				

By default, the table lists all metadata labels created in the selected partition that are more than one year old and that are not deployed or associated with a sandbox.

4. To search for a particular label or labels, you can:
 - For **Label Name**, select an operator and enter the filter criteria. The characters are case sensitive. You can use the following wildcards:
 - Percent (%): Matches any number of characters
 - Underscore (_): Matches a single character
 - Backslash (\): Used as an escape character for the wildcards
 For example, the string `postDeployLabel%` returns any label beginning with `postDeployLabel`. As a result, it displays labels associated with a deployed MAR.
 - For **Age**, enter a number, such as 2. (The only operator available is Older Than.)
 - For **Age (units)**, select a unit, such as Hours, Days, Weeks, Months, Years. The only operator available is Equals.
5. Click **Search**.
6. By default, labels associated with sandboxes and deployed applications are not shown. To display those labels, select **Sandboxes** or **Deployment** or both. Note the following:
 - You cannot delete a label associated with a sandbox.
 - If you select **Deployment**, the labels that are associated with MAR deployments are displayed.
7. Select the label and click **Delete Selected**.
8. In the confirmation box, click **OK**.

If you want to purge all unused labels, for a particular deployed application:

1. Select **Deployment**.
2. Filter by name, using the string `postDeployLabel_application_name%`.
3. Select all but the latest (which is in use) to delete. (The most recent label---the one that is currently being used---is listed first.)
4. Click **Delete Selected**.

14.3.12.4.2 Purging Metadata Labels Using WLST You can purge metadata labels that match the given pattern or age, using the WLST command `purgeMetadataLabels`. The command purges the labels that match the criteria specified, but it does not delete the metadata documents that were specified by the labels.

For example, to purge all metadata labels that match the specified `namePattern` and that are older than 30 minutes:

```
purgeMetadataLabels(repository='mds-myRepos', partition='partition1',
                    namePattern='prod*', olderThanInMin='30')
Location changed to domainRuntime tree. This is a read-only tree with DomainMBean
as the root.
For more help, use help(domainRuntime)
```

Executing operation: `purgeMetadataLabels`.

The following metadata labels were purged:
`repository=mds-soa,partition=partition1,namePattern=prod*,olderThanInMin=30:`

14.3.12.5 Deleting Metadata Labels

To delete a specified metadata label, you use the WLST command `deleteMetadataLabel`. For example, to delete a label named `prod1` for the application `my_mds_app`, use the following command:

```
deleteMetadataLabel(application='my_mds_app', server='server1', name='prod1')
```

If the application has more than one version, you must use the `applicationVersion` parameter to specify the version.

To find the labels associated with an application, use the `listMetadataLabels` command, as described in [Section 14.3.12.2](#).

14.4 Managing Metadata Repository Schemas

The following topics describe how to manage the metadata repository schemas:

- [Changing Metadata Repository Schema Passwords](#)
- [Changing the Character Set of the Metadata Repository](#)

14.4.1 Changing Metadata Repository Schema Passwords

The schema passwords are stored in the database. Note that passwords expire after a period of time. For example, for an 11g Oracle Database, by default, the passwords expire after 180 days.

For most components, you only need to change the password in the database. However, for Oracle Platform Security Services, you need to take additional steps.

This section contains the following topics:

- [Changing the Schema Passwords for Most Components](#)
- [Changing the Schema Password for Oracle Platform Security Services](#)

14.4.1.1 Changing the Schema Passwords for Most Components

To change the schema password of most components, you change the password in the database.

For example, to change the password of the schema OFM_MDS:

1. Connect to the database using SQL*Plus. Connect as a user with SYSDBA privileges.
2. Issue the following command:

```
SQL> ALTER USER schema IDENTIFIED BY new_password;
COMMIT;
```

For example, to change the OFM_MDS password to abc123:

```
SQL> ALTER USER OFM_MDS IDENTIFIED BY abc123;
COMMIT;
```

3. If you change the MDS Repository schema password, you must change the password for the corresponding MDS Repository data source, using Oracle WebLogic Server Administration Console:
 - a. From Domain Structure, expand **Services**, then **Data Sources**.
 - b. Click the data source that is related to the MDS Repository.
 - c. Click the Configuration tab, then the Connection Pool tab.
 - d. For **Password**, enter the new password.
 - e. Click **Save**.
 - f. Restart the Managed Servers that consume the data source.

14.4.1.2 Changing the Schema Password for Oracle Platform Security Services

To change the schema password for Oracle Platform Security Services:

1. Connect to the database using SQL*Plus. Connect as a user with SYSDBA privileges.
2. Issue the following command:

```
SQL> ALTER USER schema IDENTIFIED BY new_password;
COMMIT;
```

Be sure to issue the commit command before proceeding to the next step.

3. Run the WLST command `modifyBootStrapCredential` to update the JPS configuration file.
 - a. Invoke WLST from the following directory:

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

- b. Specify the full path to the JPS configuration file in the `modifyBootStrapCredentials` command. For example:

```
modifyBootStrapCredential(jpsConfigFile='/scratch/oracle//config/domains/so
a_domain/config/fmwconfig/jps-config.xml',username='schema_
username',password='password')
```


At this point, the Administration Server can be started, however, the log file will show the following exception:

```
####<Jun 30, 2014 2:15:09 PM CEST> <Error> <Deployer> <deployer>
<AdminServer> <[ACTIVE] ExecuteThread: '3' for queue:
'weblogic.kernel.Default
(self-tuning)'\> <<WLS Kernel>> <>
<f9d07f66-36d0-462e-83fd-6ca40ac15a8a-00000004> <1402936508655>
<BEA-149205>
<Failed to initialize the application "opss-data-source" due to error
weblogic.application.ModuleException:
weblogic.common.resourcepool.ResourceSystemException:
Could not connect to 'oracle.jdbc.OracleDriver'.
```

The returned message is: ORA-01017: invalid username/password; logon denied.

To avoid this error, execute next step.

4. Update the data source configuration, as described in [Section 14.4.1.1](#), step 3.

14.4.2 Changing the Character Set of the Metadata Repository

For information about changing the character set of metadata repository that is stored in an Oracle Database, see *Oracle Database Globalization Support Guide*:

<http://www.oracle.com/technetwork/database/enterprise-edition/documentation/index.html>

Oracle recommends using Unicode for all new system deployments. Deploying your systems in Unicode offers many advantages in usability, compatibility, and extensibility. Oracle Database enables you to deploy high-performing systems faster and more easily while utilizing the advantages of Unicode. Even if you do not need to support multilingual data today, nor have any requirement for Unicode, it is still likely to be the best choice for a new system in the long run and ultimately saves time and money and gives you competitive advantages in the long term.

When storing the metadata in a SQL Server database, if the character set being considered for your locale is not case neutral, the case-sensitive collation must be selected during the creation of the database instance. Unicode support is the default when creating the MDS schema for SQL Server using RCU. You may overwrite this default to use non-unicode schema if that meets your requirements.

14.5 Purging Data

When the amount of data in Oracle Fusion Middleware databases grows very large, maintaining the databases can become difficult and can affect performance. In some cases, Oracle Fusion Middleware automatically purges data. In other cases, Oracle Fusion Middleware provides methods to manage growth, including scripts to purge data that can accumulate over time and that can affect performance.

Many of the Oracle Fusion Middleware components provide scripts written as PL/SQL procedures to purge the data. The scripts are located in:

`ORACLE_HOME/common/sql/component-name_purge_purgetype.sql`

For example, a script that purges logs for Oracle Business Process Management is located in:

`ORACLE_HOME/common/sql/bpm_purge_logs.sql`

Table 14–2 provides pointers to information about purging data for Oracle Fusion Middleware components.

Table 14–2 Purging Data Documentation

Component	Description
Oracle Application Development Framework	See "Cleaning Up Temporary Storage Tables" in <i>Developing Fusion Web Applications with Oracle Application Development Framework</i> .
Oracle Application Development Framework Business Components	Use the following script to purge rows in the database used by Oracle ADF Business Components to store user session state and temporary persistent collections: <code>ORACLE_HOME/oracle_common/common/sql/adfbc_purge_statesnapshots.sql</code> The PS_TXN table is automatically purged.
Oracle SOA Suite	See "Managing Database Growth" in the <i>Administering Oracle SOA Suite and Oracle Business Process Management Suite</i> .
Oracle WebLogic Server: Oracle Infrastructure Web Services	Use the following script to purge data if WS-RM uses a database store: <code>ORACLE_HOME/oracle_common/common/sql/ows_purge_wsrn_msgs.sql</code>
Oracle WebLogic Server: JAXWS Web Services	Clean up the Web service persistence store, as described in "Cleaning Up Web Service Persistence" in <i>Developing JAX-WS Web Services for Oracle WebLogic Server</i> . Use the defaultMaximumObjectLifetime field of the WebServicePersistenceMBean to set the maximum lifetime of the objects. See "Understanding WebLogic Server MBeans" in <i>Developing Custom Management Utilities Using JMX for Oracle WebLogic Server</i> .
Oracle WebLogic Server: Stateful EJBs	No configuration required. Automatically purges data.
Oracle WebLogic Server: JMS	See "Configuring Basic JMS System Resources" and "Managing JMS Messages" in <i>Administering JMS Resources for Oracle WebLogic Server</i> . Also see "Tuning WebLogic JMS" in <i>Tuning Performance of Oracle WebLogic Server</i> .
Oracle WebLogic Server: Session persistence for JDBC or file-based data sources	No configuration required. Automatically purges data.
MDS Repository	See Section 14.3.11 for information on automatically and manually purging data.
Oracle Web Services Manager	No configuration required. Automatically purges data.

In certain circumstances, you can consider using Oracle Scheduler to automate the running of the scripts. For example, you may want to set up a scheduled job to purge the last 14 days for completed instances.

In certain circumstances, you can consider using Oracle Scheduler to automate the running of the scripts. For example, you may want to set up a scheduled job to purge the last 14 days for completed instances for Oracle SOA Suite.

Oracle Scheduler, an enterprise job scheduler, is part of Oracle Database. Oracle Scheduler is implemented by the procedures and functions in the DBMS_SCHEDULER PL/SQL package. For information about Oracle Scheduler, see "Oracle Scheduler Concepts" and "Creating, Running, and Managing Jobs" in the *Oracle Database Administrator's Guide*.

14.5.1 Purging Oracle Infrastructure Web Services Data

Use the following script to purge data if WS-RM uses a database store:

```
ORACLE_HOME/oracle_common/common/sql/ows_purge_wsrn_msgs.sql
```

Changing Network Configurations

This chapter provides procedures for changing the network configuration, such as the host name, domain name, or IP address, of an Oracle Fusion Middleware host and the Oracle database that Oracle Fusion Middleware uses. It also includes information about using the IPv6 protocol with Oracle Fusion Middleware.

It contains the following sections:

- [Section 15.1, "Changing the Network Configuration of Oracle Fusion Middleware"](#)
- [Section 15.2, "Changing the Network Configuration of a Database"](#)
- [Section 15.3, "Moving Between On-Network and Off-Network"](#)
- [Section 15.4, "Changing Between a Static IP Address and DHCP"](#)
- [Section 15.5, "Using IPv6"](#)

15.1 Changing the Network Configuration of Oracle Fusion Middleware

This section describes how to change the host name, domain name, IP address, or any combination of these, of a host that contains the following installation types:

- Oracle WebLogic Server and Java components. When you change the host name, domain name, or IP address of Oracle WebLogic Server, you also automatically change the information for Java components, such as Oracle SOA Suite components, that are deployed to Oracle WebLogic Server.
- Oracle HTTP Server. You can change the host name or the IP address.

For information about moving your environment to a different system, see [Chapter 20](#).

The following topics describe how to change the host name, domain name, or IP address:

- [Changing the Network Configuration of an Administration Server](#)
- [Changing the Network Configuration of a Managed Server](#)
- [Changing the Network Configuration of Oracle HTTP Server](#)

15.1.1 Changing the Network Configuration of an Administration Server

You can change the network configuration of an Administration Server using WLST commands:

1. Stop the Administration Server.
2. For the Administration Server, set the machine with the new host name, using the following WLST command, in offline mode:

```
wls:/offline> readDomain('DOMAIN_HOME')
wls:/offline/sampledomain> cd ('/Machine/newhostname')
wls:/offline/sampledomain> machine = cmo
wls:/offline/sampledomain> cd ('/Server/AdminServer')
wls:/offline/sampledomain> set('Machine', machine)
wls:/offline/sampledomain> updateDomain()
wls:/offline/sampledomain> exit()
```

3. Set the listen port for the Administration Server:

```
wls:/offline/sampledomain> readDomain('DOMAIN_HOME')
wls:/offline/sampledomain> cd('/Server/AdminServer')
wls:/offline/sampledomain> cmo.setListenPort(8001)
wls:/offline/sampledomain> updateDomain()
wls:/offline/sampledomain> exit()
```

4. Start the Administration Server.

15.1.2 Changing the Network Configuration of a Managed Server

You can change the network configuration of a Managed Server using the Oracle WebLogic Server Administration Console.

To change the host name, domain name, or IP address of a Managed Server:

1. Display the Administration Console, as described in [Section 2.3.1](#).
2. In the Change Center, click **Lock & Edit**.
3. Create a machine, which is a logical representation of the computer that hosts one or more WebLogic Servers, and point it to the new host. (From the Home page, select **Machines**. Then, click **New**.) Follow the directions in the Administration Console help.

You must disable Host Name Verification on Administration Servers that access Node Manager, as described in "Using Hostname Verification" in *Administering Security for Oracle WebLogic Server*.

4. Restart the Administration Server.
5. Change the Managed Server configuration to point to the new machine:
 - a. From the left pane of the Console, expand **Environment** and then **Servers**. Then, select the name of the server.
 - b. Select the **Configuration** tab, then the **General** tab. In the **Machine** field, select the machine to which you want to assign the server.
 - c. Change **Listen Address** to the new host.
Click **Save**.
6. Start the Managed Server. You can use the Oracle WebLogic Server Administration Console, WLST, or the following command:

```
DOMAIN_NAME/bin/startManagedWeblogic.sh managed_server_name
admin_url
```

The Managed Server connects to the Administration Server and updates its configuration changes.

15.1.3 Changing the Network Configuration of Oracle HTTP Server

To change the network configuration of Oracle HTTP Server in a WebLogic domain or a standalone domain:

1. Perform a backup of your environment before you start this procedure. See [Chapter 17](#).
2. Update your operating system with the new host name, domain name, IP address, or any combination of these. Consult your operating system documentation for information on how to perform the following steps.
 - a. Make the updates to your operating system to properly change the host name, domain name, or IP address.
 - b. Restart the host, if necessary for your operating system.
 - c. Verify that you can ping the host from another host in your network. Be sure to ping using the new host name to ensure that everything is resolving properly.

3. Stop Node Manager as described in [Section 4.2.2](#).

4. Stop Oracle HTTP Server. For example:

```
./stopComponent.sh ohs1
```

5. Change to the following directory:

```
DOMAIN_HOME/config/fmwconfig/components/OHS/ohs_component_name
```

6. For each configuration file (files ending in .conf):

- Search for the old canonical host name (for example oldhost.example.com) and replace it with the new canonical host name (for example newhost.example.com).
- Search for the old short host name (for example oldhost) and replace it with the new short host name (for example newhost).
- Search for the old IP address and replace it with the new IP address.

7. Restart Node Manager:

```
DOMAIN_HOME/bin/startNodeManager.sh
```

8. Restart Oracle HTTP Server:

```
./startComponent.sh ohs1
```

15.2 Changing the Network Configuration of a Database

This section describes how to change the host name, domain name, or IP address of a host that contains a database that contains the metadata for Oracle Fusion Middleware components:

The following tasks describe the procedure:

- [Task 1, "Stop All Oracle Fusion Middleware Components"](#)
- [Task 2, "Shut Down the Database"](#)
- [Task 3, "Change the Network Configuration"](#)
- [Task 4, "Change References to the Network Configuration"](#)

- [Task 5, "Start the Database"](#)
- [Task 6, "Change the System Data Source"](#)
- [Task 7, "Restart Your Environment"](#)

Task 1 Stop All Oracle Fusion Middleware Components

Stop all components that use the database, even if they are on other hosts. Stop the Administration Server, the Managed Servers, and all components, as described in [Chapter 4](#).

Task 2 Shut Down the Database

Prepare your host for the change by stopping the database:

1. Set the ORACLE_HOME and ORACLE_SID environment variables.
2. Shut down the listener and database:

```
lsnrctl stop

sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> shutdown
SQL> quit
```

3. Verify that all Oracle Fusion Middleware processes have stopped.
4. To ensure that Oracle Fusion Middleware processes do not start automatically after a restart of the host, disable any automated startup scripts you may have set up, such as `/etc/init.d` scripts.

Task 3 Change the Network Configuration

If you are changing the host name, domain name, or IP address, update your operating system with the new names or IP address, restart the host, and verify that the host is functioning properly on your network. Consult your operating system documentation for information on how to perform the following steps:

1. Make the updates to your operating system to properly change the host name, domain name or IP address.
2. Restart the host, if required by your operating system.
3. Verify that you can ping the host from another host in your network. Be sure to ping using the new host name, domain name, or IP address to ensure that everything is resolving properly.

Task 4 Change References to the Network Configuration

You must modify files that contain the host name, domain name, or IP address, depending on the components that you are using. The following lists some of the files that you may need to modify to change references to the new host name, domain name or IP address:

- `tnsnames.ora`, which is located in:
`ORACLE_HOME/network/admin/tnsnames.ora`
- `listener.ora`, which is located in:
(UNIX) `ORACLE_HOME/network/admin/listener.ora`
(Windows) `ORACLE_HOME\network\admin\listener.ora`

- For Oracle HTTP Server, edit the `httpd.conf` file, making the following changes:
 - Update the `Listen` directive with the new host name or IP address and port (if the production environment Oracle HTTP Server is using a different port).
 - Update the `VirtualHost` directive, if the host name, IP address, or port number is defined, with the new values for the production environment.
 - Update any other nondefault directives that were configured at the test environment and have topological (host name, IP address, port number) or other machine-specific information.
- For Oracle HTTP Server, the `PlsqlDatabaseConnectionString` in the `dads.conf` file
- For Oracle HTTP Server, if you use `mod_oradav`, the `ORACONNECTSN` parameter in the `mod_oradav.conf` file
- For Oracle HTTP Server, if you use `mod_plsql`, the `PlsqlDatabaseConnectionString` attribute in the `dads.conf` file
- For Oracle HTTP Server, if you use `mod_wl_ohs`, update the `mod_wl_ohs.conf` file
 - Update the `WebLogicHost`, `WebLogicPort`, or `WebLogicCluster` directives with the host name, IP address, and port number.

This is not an exhaustive list. See [Chapter 20](#) for additional information about files used by components. That chapter describes how to move components, including a database, from a test to a production system, in effect changing the host name.

Task 5 Start the Database

Start the database:

1. Log in to the host as the user that installed the database.
2. Set the `ORACLE_HOME` and `ORACLE_SID` environment variables.
3. On UNIX systems, set the `LD_LIBRARY_PATH`, `LD_LIBRARY_PATH_64`, `LIB_PATH`, or `SHLIB_PATH` environment variables to the proper values. The actual environment variables and values that you must set depend on the type of your UNIX operating system.
4. Start the database and listener:

```
sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> startup
SQL> quit
```

```
lsnrctl start
```

Task 6 Change the System Data Source

Change the system data source to use the new host name, domain name, or IP address for the database, as described in [Section 14.3.4](#).

Task 7 Restart Your Environment

Start the components that use the database:

1. Start all components that use the database, even if they are on other hosts. Start the Administration Server, the Managed Servers, and all components, as described in [Chapter 4](#).
2. If you disabled any processes from automatically starting Oracle Fusion Middleware at the beginning of this procedure, enable them.

15.3 Moving Between On-Network and Off-Network

This section describes how to move an Oracle Fusion Middleware host on and off the network. The following assumptions and restrictions apply:

- The host must contain an instance that does not use an Infrastructure, or both the middle-tier instance and Infrastructure must be on the same host.
- DHCP must be used in loopback mode. Refer to the *Oracle Fusion Middleware System Requirements and Specifications* document for more information.
- Only IP address change is supported; the host name must remain unchanged.
- Hosts in DHCP mode should not use the default host name (`localhost.localdomain`). The hosts should be configured to use a standard host name and the loopback IP should resolve to that host name.
- A loopback adapter is required for all off-network installations (DHCP or static IP). Refer to the *Planning an Installation of Oracle Fusion Middleware* for more information.

15.3.1 Moving from Off-Network to On-Network (Static IP Address)

This procedure assumes you have installed Oracle Fusion Middleware on a host that is off the network, using a standard host name (not `localhost`), and would like to move on to the network and use a static IP address. The IP address may be the default loopback IP, or any standard IP address.

To move on to the network, you can simply connect the host to the network. No updates to Oracle Fusion Middleware are required.

15.3.2 Moving from Off-Network to On-Network (DHCP)

This procedure assumes you have installed on a host that is off the network, using a standard host name (not `localhost`), and would like to move on to the network and use DHCP. The IP address of the host can be any static IP address or loopback IP address, and should be configured to the host name.

To move on to the network:

1. Connect the host to the network using DHCP.
2. Configure the host name to the loopback IP address only.

15.3.3 Moving from On-Network to Off-Network (Static IP Address)

Follow this procedure if your host is on the network, using a static IP address, and you would like to move it off the network:

1. Configure the `/etc/hosts` file so the IP address and host name can be resolved locally.
2. Take the host off the network.

There is no need to perform any steps to change the host name or IP address.

15.4 Changing Between a Static IP Address and DHCP

This section describes how to change between a static IP address and DHCP. The following assumptions and restrictions apply:

- The host must contain all Oracle Fusion Middleware components, including Identity Management components, and any database associated with those components. That is, the entire Oracle Fusion Middleware environment must be on the host.
- DHCP must be used in loopback mode. Refer to *Planning an Installation of Oracle Fusion Middleware* for more information.
- Only IP address change is supported; the host name must remain unchanged.
- Hosts in DHCP mode should not use the default host name (`localhost.localdomain`). The hosts should be configured to use a standard host name and the loopback IP should resolve to that host name.

15.4.1 Changing from a Static IP Address to DHCP

To change a host from a static IP address to DHCP:

1. Configure the host to have a host name associated with the loopback IP address before you convert the host to DHCP.
2. Convert the host to DHCP. There is no need to update Oracle Fusion Middleware.

15.4.2 Changing from DHCP to a Static IP Address

To change a host from DHCP to a static IP address:

1. Configure the host to use a static IP address.
2. There is no need to update Oracle Fusion Middleware.

15.5 Using IPv6

Oracle Fusion Middleware supports Internet Protocol Version 4 (IPv4) and Internet Protocol Version 6 (IPv6.) Among other features, IPv6 supports a larger address space (128 bits) than IPv4 (32 bits), providing an exponential increase in the number of computers that can be addressable on the Web.

An IPv6 address is expressed as 8 groups of 4 hexadecimal digits. For example:

```
2001:0db8:85a3:08d3:1319:8a2e:0370:7334
```

For information about the support for IPv6 by Oracle Fusion Middleware components, see *Oracle Fusion Middleware System Requirements and Specifications*.

The following topics provide more information about configuring Oracle Fusion Middleware components for IPv6:

- [Configuring Oracle HTTP Server for IPv6](#)
- [Using Dual Stack with Oracle SOA Suite and Fusion Middleware Control](#)

15.5.1 Configuring Oracle HTTP Server for IPv6

To configure Oracle HTTP Server to communicate using IPv6, you modify configuration files in the following directory:

```
(UNIX) DOMAIN_HOME/config/fmwconfig/components/OHS/ohs_name
(Windows) DOMAIN_HOME\config\fmwconfig\components\OHS\ohs_name
```

For example, to configure Oracle HTTP Server to communicate with Oracle WebLogic Server on hosts that are running IPv6, you configure `mod_wl_ohs`. You edit the configuration files in the following directory:

```
DOMAIN_HOME/config/fmwconfig/components/OHS/instances/ohs1
```

In the files, specify either the resolvable host name or the IPv6 address in one of the following parameters:

```
WebLogicHost hostname | [IPaddress]
WebCluster [IPaddress_1]:portnum1, [IPaddress_2]:portnum2, [IPaddress_3]:portnum3,
...
```

You must enclose the IPv6 address in brackets.

Any errors are logged in the Oracle HTTP Server logs. To generate more information, set the `mod_weblogic` directives `Debug All` and `WLLogFile` path. Oracle HTTP Server logs module-specific messages.

Note: In previous versions, Oracle HTTP Server contained restrictions about using dynamic clusters with IPv6 nodes. For example, the Oracle HTTP Server plug-in for Oracle WebLogic Server had limited IPv6 support in that the DSL (dynamic server list) feature of the plug-in was not supported; only the static configuration of server lists was supported (`DynamicServerList=OFF`). Those restrictions have been lifted.

15.5.2 Using Dual Stack with Oracle SOA Suite and Fusion Middleware Control

Oracle SOA Suite supports a dual-stack configuration. However, when you use Fusion Middleware Control with Oracle SOA Suite, you must specify the protocol in the following file. Otherwise, Fusion Middleware Control may not work correctly.

```
DSOMAIN_HOME/bin/startWebLogic.sh
```

In the file, add the following line, specifying the IP protocol after the line `${DOMAIN_HOME}/bin/setDomainEnv.sh`:

```
DOMAIN_HOME/bin JAVA_OPTIONS="${JAVA_OPTIONS} -Djava.net.preferIPv4Stack=true"
```

Part VII

Advanced Administration: Backup and Recovery

Backup and recovery refers to the various strategies and procedures involved in guarding against hardware failures and data loss, and reconstructing data should loss occur. This part describes how to back up and recover Oracle Fusion Middleware.

It contains the following chapters:

- [Chapter 16, "Introducing Backup and Recovery"](#)
- [Chapter 17, "Backing Up Your Environment"](#)
- [Chapter 18, "Recovering Your Environment"](#)

Introducing Backup and Recovery

This chapter provides an introduction to backing up and recovering Oracle Fusion Middleware, including backup and recovery recommendations for Oracle Fusion Middleware components.

It contains the following sections:

- [Section 16.1, "Understanding Oracle Fusion Middleware Backup and Recovery"](#)
- [Section 16.2, "Oracle Fusion Middleware Directory Structure"](#)
- [Section 16.3, "Tools to Use for Backup and Recovery"](#)
- [Section 16.4, "Backup and Recovery Recommendations for Oracle Fusion Middleware Components"](#)
- [Section 16.5, "Assumptions and Restrictions"](#)

16.1 Understanding Oracle Fusion Middleware Backup and Recovery

An Oracle Fusion Middleware environment can consist of different components and configurations. A typical Oracle Fusion Middleware environment contains an Oracle WebLogic Server domain with Java components, such as Oracle SOA Suite, and a WebLogic Server domain with Identity Management components.

The installations of an Oracle Fusion Middleware environment are interdependent in that they contain configuration information, applications, and data that are kept in synchronization. For example, when you perform a configuration change, information in configuration files is updated. When you deploy an application, you might deploy it to all Managed Servers in a domain or cluster.

It is, therefore, important to consider your entire Oracle Fusion Middleware environment when performing backup and recovery. You should back up your entire Oracle Fusion Middleware environment at once, then periodically. If a loss occurs, you can restore your environment to a consistent state.

The following topics describe concepts that are important to understanding backup and recovery:

- [Impact of Administration Server Failure](#)
- [Managed Server Independence \(MSI\) Mode](#)
- [Configuration Changes in Managed Servers](#)

See Also: *Understanding Oracle Fusion Middleware* for conceptual information about Oracle WebLogic Server domains, the Administration Server, Managed Servers and clusters, and Node Manager.

16.1.1 Impact of Administration Server Failure

The failure of an Administration Server does not affect the operation of Managed Servers in the domain but it does prevent you from changing the domain's configuration. If an Administration Server fails because of a hardware or software failure on its host computer, other server instances on the same computer may be similarly affected.

If an Administration Server for a domain becomes unavailable while the server instances it manages—clustered or otherwise—are running, those Managed Servers continue to run. Periodically, these Managed Servers attempt to reconnect to the Administration Server. For clustered Managed Server instances, the load balancing and failover capabilities supported by the domain configuration continue to remain available.

When you first start a Managed Server, it must be able to connect to the Administration Server to retrieve a copy of the configuration. Subsequently, you can start a Managed Server even if the Administration Server is not running. In this case, the Managed Server uses a local copy of the domain's configuration files for its starting configuration and then periodically attempts to connect with the Administration Server. When it does connect, it synchronizes its configuration state with that of the Administration Server.

16.1.2 Managed Server Independence (MSI) Mode

A Managed Server maintains a local copy of the domain configuration. When a Managed Server starts, it contacts its Administration Server to retrieve any changes to the domain configuration that were made since the Managed Server was last shut down. If a Managed Server cannot connect to the Administration Server during startup, it can use its locally cached configuration information—this is the configuration that was current at the time of the Managed Server's most recent shutdown. A Managed Server that starts without contacting its Administration Server to check for configuration updates is running in Managed Server Independence (MSI) mode. By default, MSI mode is enabled. However a Managed Server cannot be started even in MSI mode for the first time if the Administration Server is down due to non-availability of the cached configuration.

16.1.3 Configuration Changes in Managed Servers

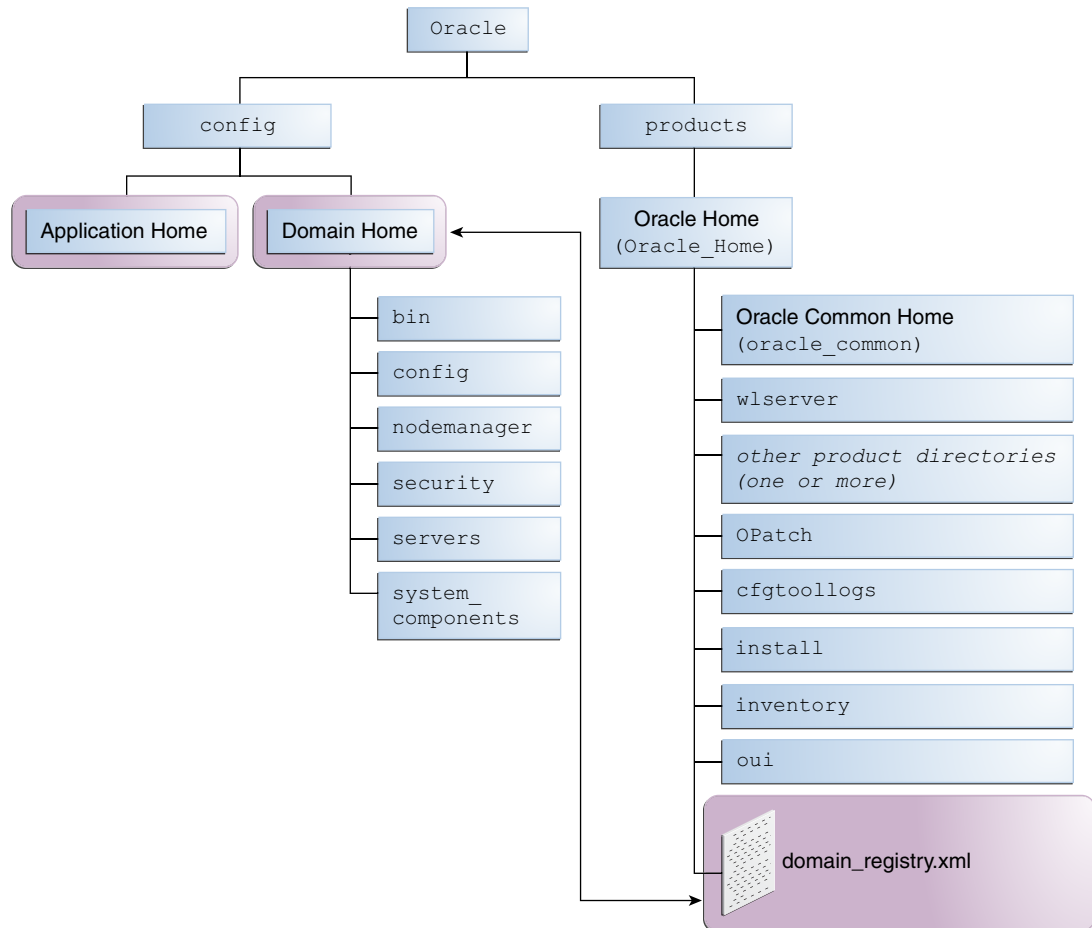
Configuration changes are updated in a Managed Server during the following events:

- On each Managed Server restart, the latest configuration is retrieved from the Administration Server. This happens even when Node Manager is down on the node where the Managed Server is running. If the Administration Server is unavailable during the Managed Server restart and if the MSI (Managed Server Independence) mode is enabled in the Managed Server, it starts by reading its local copy of the configuration and synchronizes with the Administration Server when it is available. By default MSI mode is enabled.
- Upon activating every administrative change such as configuration changes, deployment or redeployment of applications, and topology changes, the Administration Server pushes the latest configuration to the Managed Server. If

the Managed Server is not running, the Administration Server pushes the latest version of the configuration to the Managed Server when it does start.

16.2 Oracle Fusion Middleware Directory Structure

The following shows a simplified view of the Oracle Fusion Middleware directory structure when you have installed the Oracle Fusion Middleware Infrastructure:



16.3 Tools to Use for Backup and Recovery

To backup or recover your Oracle Fusion Middleware environment, you can use:

- File copy utilities such as `copy`, `xcopy`, `tar`, or `jar`. Make sure that the utilities:
 - Preserve symbolic links
 - Support long file names
 - Preserve the permissions, timestamps, and ownership of the files

When you backup and restore the files, use your preferred tool. For example:

- On Windows, for online backup and recovery, use `copy` or `xcopy`; for offline backup and recovery, use `copy`, `xcopy`, or `jar`. Do not use Winzip because it does not work with long filenames or extensions.

Note that for some versions of Windows, any file name with more than 256 characters fails. You can use the `xcopy` command with the following switches to work around this issue:

```
xcopy /s/e "C:\Temp\*.*)" "C:\copy"
```

See the `xcopy` help for more information about syntax and restrictions.

- On Linux and UNIX, use `tar`.

If you want to retain your backups for a longer duration, you may want to back up to tape, for example using Oracle Secure Backup.

- Oracle Recovery Manager (RMAN) to back up or recover database-based metadata repositories and any databases used by Oracle Fusion Middleware. With RMAN, you can perform full backups or incremental backups. See *Oracle Database Backup and Recovery User's Guide* for information about using RMAN to back up or recover a database.

You can also configure Oracle WebLogic Server to make backup copies of the configuration files. This facilitates recovery in cases where configuration changes need to be reversed or in the unlikely case that configuration files become corrupted. When the Administration Server starts, it saves a `.jar` file named `config-booted.jar` that contains the configuration files. When you make changes to the configuration files, the old files are saved in the `configArchive` directory under the domain directory, in a `.jar` file with a sequentially numbered name such as `config-1.jar`. However, the configuration archive is always local to the Administration Server host. It is a best practice to back up the archives to an external location.

16.4 Backup and Recovery Recommendations for Oracle Fusion Middleware Components

[Table 16–1](#) describes what you must back up and recover for each Oracle Fusion Middleware component. Note the following:

- If the component has a database dependency listed in the table, back up and recover the database using RMAN, as described in the *Oracle Database Backup and Recovery User's Guide*.
- For backup, back up the entity listed in the table, as described in [Section 17.3](#).
- For recovery, depending on what has failed, you may need to recover the following, as described in [Chapter 18](#):
 - The domain, which, for some components, can be either a WebLogic Server domain (see [Section 18.2.2](#)) or a standalone domain (see [Section 18.2.3](#)).
 - The Administration Server configuration: See [Section 18.2.4](#).
 - A Managed Server: See [Section 18.2.5](#).
 - A cluster: See [Section 18.2.7](#).
 - Applications: See [Section 18.2.8](#).

After a loss of host, you may need to recover the following:

- The domain, which, for some components, can be either a WebLogic Server domain (see [Section 18.3.1](#)) or a standalone domain (see [Section 18.3.2](#)).
- The Administration Server host: See [Section 18.3.3](#).
- The Managed Server host: See [Section 18.3.4](#).

Table 16–1 describes the backup and recovery recommendations for Oracle Fusion Middleware components.

Table 16–1 Backup and Recovery Recommendations

Component	Database Dependencies	Backup Recommendation	Recovery Recommendation	Additional Information
Oracle WebLogic Server	By default, does not depend on any database repository. However, applications deployed on Oracle WebLogic Server may use databases as data sources.	The Oracle home and the Administration Server domain directory	The entity that has failed	If you use Whole Server Migration, see Section 18.2.2.1 .
Oracle WebLogic Server JMS	Only if JMS is database-based	The Oracle home and the Administration Server domain directory	The entity that has failed	See Section 16.4.1 .
Oracle Web Services Manager	If a database-based MDS Repository is used, the MDS schema.	The Oracle home and the Administration Server domain directory. If Oracle WSM uses a file-based MDS repository, back it up using a file copy mechanism.	The Managed Server If Oracle WSM uses a file-based MDS repository, restore it from backup.	NA
Oracle Platform Security Services	If a database-based Oracle Platform Security repository is used, the OPSS schema. If an Oracle Internet Directory based repository is used, an Oracle Internet Directory repository.	The Oracle home and the Administration Server domain directory. Back up Oracle Internet Directory if Oracle Platform Security uses an Oracle Internet Directory based repository.	The files listed in Section 18.2.6.1 .	
Oracle User Messaging Service	UMS schema	The Oracle home and the domain, which can be either a standalone domain or the Oracle WebLogic Server domain.	The domain, which can be either a standalone domain or the Oracle WebLogic Server domain	Make configuration changes as described in Section 18.3.5.5.1 or Section 18.3.5.5.2 .
Oracle HTTP Server	None	The Oracle home and the domain, which can be either a standalone domain or the Oracle WebLogic Server domain.	The Administration Server domain directory	NA

Table 16–1 (Cont.) Backup and Recovery Recommendations

Component	Database Dependencies	Backup Recommendation	Recovery Recommendation	Additional Information
Oracle SOA Suite	MDS and SOAINFRA schemas	The Oracle home and the Administration Server domain directory	The entity that has failed	For loss of host, see Section 18.3.5.4 . See Section 16.4.2 for information about backing up and recovering the database.
Oracle B2B	MDS schema	The Administration Server domain directory, the Oracle home, and the product home if changes are made to the Oracle B2B configuration file	The Managed Server	See Section 18.2.6.2 for information about the file Xengine.tar.gz.
Oracle BPEL Process Manager	MDS and SOAINFRA schemas	The Oracle home and the Administration Server domain directory	The entity that has failed	See Section 16.4.2 for information about backing up and recovering the database.
Oracle Business Activity Monitoring	MDS and SOAINFRA schemas	The Oracle home, the Administration Server domain directory, the Managed Server directory.	The Managed Server or the Oracle home, or both, depending on the extent of failure	NA
Oracle Business Process Management	MDS schema	The Administration Server domain directory and the same data as Oracle BPEL Process Manager, as described in Section 16.4.2 .	The same data as Oracle BPEL Process Manager and the Managed Server	NA
Oracle Business Rules	MDS schema	The Oracle home and the Administration Server domain directory	The Managed Server where the soa-infra application is deployed	NA
Oracle Managed File Transfer	MFT and MDS and schemas	The Oracle home and the Administration Server domain directory	The entity that has failed	
Oracle Service Bus	If its reporting feature is enabled, Oracle Service Bus creates two tables, WLI_QS_REPORT_DATA and WLI_QS_REPORT_ATTRIBUTE, in a user-specified schema.	The Oracle home and the Administration Server domain directory	The Managed Server	

Table 16–1 (Cont.) Backup and Recovery Recommendations

Component	Database Dependencies	Backup Recommendation	Recovery Recommendation	Additional Information
Oracle Mediator	MDS and SOAINFRA schemas	The Oracle home and the Administration Server domain directory	The Managed Server where the soa-infra application is deployed	
Oracle Enterprise Scheduler	ESS schema	The Oracle home and the Administration Server domain directory	The entity that has failed	NA
Oracle Event Processing	MDS schema, which stores the .cplx files packaged in a MAR	The Oracle home and the Administration Server domain directory	The Managed Server	NA
Oracle Data Integrator	ODI_REPO schema	The Oracle home, the domain if Oracle Data Integrator is installed in a domain, and the ODI_Oracle_Home/oracledi/agent folder for each machine where a standalone agent is installed	The Managed Server or the Oracle home, or both. If your environment contains the Oracle Data Integrator Standalone Agent or Oracle Data Integrator for Developers, restore the Oracle home, as described in Section 18.2.1 . If your environment contains Oracle Data Integrator deployed in a Managed Server, restore the Managed Server, as described in Section 18.2.5 .	To recover from loss of host, see Section 18.3.5.6 .
Oracle Data Service Integrator	MDS schema	The Oracle home and the Administration Server domain directory	The Administration Server domain	NA

16.4.1 Backup and Recovery Considerations for Oracle WebLogic Server JMS

If you are using file-based JMS, use storage snapshot techniques for taking consistent online backups. Alternatively, you can use a file-system copy to perform an offline backup.

If the JMS persistent store is file-based, recover it from backup. If the JMS persistent store is database-based, recover the database to the most recent point in time, if needed. Note the following:

- Always try to keep JMS data as current as possible. This can be achieved by using the point-in-time recovery capabilities of Oracle Database, recovering to the most recent time (in the case of database-based persistence) or using a highly available RAID-backed storage device (for example, SAN/NAS).
- If you are using a file-based JMS, you can use storage snapshots to recover.

- If, for whatever reason, you need to restore JMS data to a previous point in time, there are potential implications. Restoring the system state to a previous point in time not only can cause duplicate messages, but can also cause lost messages. The lost messages are messages that were enqueued before or after the system restore point time, but never processed.

Use the following procedure *before recovery* to drain messages in the JMS queue after persistent-store recovery to avoid processing duplicate messages:

Note: Do not drain and discard messages without first being certain that the messages contain no data that must be preserved. The recovered messages may include unprocessed messages with important application data, in addition to duplicate messages that have already been processed.

1. Log into the Oracle WebLogic Server Administration Console.
2. Before recovery, configure JMS server to pause Production, Insertion, and consumption operations at boot time to ensure that no new messages are produced or inserted into the destination or consumed from the destination before you drain stale messages. To do this:
 - a. Expand **Services**, then **Messaging**, and then click **JMS Servers**.
 - b. On the Summary of JMS Servers page, click the JMS server you want to configure for message pausing.
 - c. On the Configuration: General page, click **Advanced** to define the message pausing options. Select **Insertion Paused At Startup**, **Production Paused At Startup**, and **Consumption Paused At Startup**.
 - d. Click **Save**.

Use the following procedure *after recovery*:

1. After recovering the persistent store, start the Managed Servers.
2. Drain the stale messages from JMS destinations, by taking the following steps:
 - a. Expand **Services**, then **Messaging**, and then **JMS Modules**.
 - b. Select a JMS module, then select a target.
 - c. Select **Monitoring**, then **Show Messages**.
3. Click **Delete All**.
4. Resume operations, by taking the following steps:
 - a. Expand **Services**, then **Messaging**, and then **JMS Servers**.
 - b. On the Summary of JMS Servers page, click the JMS server you want to configure for message pausing.
 - c. On the Configuration: General page, click **Advanced**. Deselect **Insertion Paused At Startup**, **Production Paused At Startup**, and **Consumption Paused At Startup**.
 - d. Click **Save**.

If the store is not dedicated to JMS use, use the Oracle WebLogic Server JMS message management administrative tool. This tool can perform import, export,

move, and delete operations from the Administration Console, MBeans, and WLST.

For applications that use publish and subscribe in addition to queuing, you should manipulate topic subscriptions in addition to queues.

16.4.2 Backup and Recovery Recommendations for Oracle BPEL Process Manager

Back up the database after any configuration changes, including changes to global fault policies, callback classes for workflows and resource bundles that can potentially be outside the suitcase. Also back up the database after deploying a new composite or redeploying a composite.

Recover the database to the most recent point in time, if needed. Point-in-time recovery ensures that the latest process definitions and in-flight instances are restored. However, this may result in reexecution of the process steps. Oracle recommends that you strive for idempotent Oracle BPEL Process Manager processes. If the system contains processes that are not idempotent, you must clean them up from the dehydration store before starting Oracle Fusion Middleware. See *Administering Oracle SOA Suite and Oracle Business Process Management Suite* for more information.

Because instances obtain the process definition and artifacts entirely from the database, there is no configuration recovery needed after the database is recovered to the most current state; instances should continue to function correctly.

For redeployed composites, a database recovery ensures consistency between the dehydrated in-flight processes and their corresponding definition since the process definition is stored in database repository where dehydrated instances are also stored.

16.5 Assumptions and Restrictions

The following assumptions and restrictions apply to the backup and recovery procedures in this book. Also see the restrictions listed in [Section 17.2](#).

- Only the user who installs the product or a user who has access privileges to the directories where Oracle Fusion Middleware has been installed should be able to execute backup and recovery operations.
- If a single Managed Server and Administration Server run on different hosts and the Managed Server is not in a cluster, you must use the pack and unpack commands on the Managed Server to retrieve the correct configuration.

See Also: If you are using Cold Failover Cluster or Disaster Recovery, refer to the *Disaster Recovery Guide* for additional information.

Backing Up Your Environment

This chapter describes recommended backup strategies for Oracle Fusion Middleware and the procedures for backing up Oracle Fusion Middleware.

This chapter includes the following sections:

- [Section 17.1, "Overview of the Backup Strategies"](#)
- [Section 17.2, "Limitations and Restrictions for Backing Up Data"](#)
- [Section 17.3, "Performing a Backup"](#)
- [Section 17.4, "Creating a Record of Your Oracle Fusion Middleware Configuration"](#)

17.1 Overview of the Backup Strategies

Backup strategies enable you safeguard your data and to later recover from critical failures that involve actual data loss. The following topics describe the backup strategy:

- [Types of Backups](#)
- [Backup Artifacts](#)
- [Recommended Backup Strategy](#)

17.1.1 Types of Backups

You can back up your Oracle Fusion Middleware environment offline or online:

- An **offline backup** means that you must shut down the environment before backing up the files. When you perform an offline backup, the Administration Server and all Managed Servers in the domain should be shut down.
- An **online backup** means that you do not shut down the environment before backing up the files. To avoid an inconsistent backup, do not make any configuration changes until the backup is completed. To ensure that no changes are made in the WebLogic Server domain, lock the WebLogic Server configuration, as described in [Section 2.3.2](#).

You can perform backups on your full Oracle Fusion Middleware environment, or on the run-time artifacts, which are those files that change frequently.

To perform a full backup, you should back up the static files and directories, as well as run-time artifacts, which are described in [Section 17.1.2](#).

17.1.2 Backup Artifacts

Backup artifacts include static files and directories and run-time artifacts.

Static files and directories are those that do not change frequently. These include:

- The Oracle home (*ORACLE_HOME*). An Oracle home consists of product homes, such as the WebLogic Server home and an Oracle Common home, which contain the product binaries.

Although not recommended, it can also contain the *user_projects* directories, which contains Oracle WebLogic Server domains, which are not static files.

- OraInventory
- On Linux and UNIX, the *oraInst.loc* file, which is located in the following directory:

(Linux and IBM AIX) /etc
(Other UNIX systems) /var/opt/oracle

- On Linux and UNIX, the *oratab* file, which is located in the following directory:

/etc

- The *beahomelist* file, which is located at:

(UNIX) *user_home*/bea/beahomelist
(Windows) C:\bea\beahomelist

- On Windows, the following registry key:

HKEY_LOCAL_MACHINE\Software\oracle

In addition, for system components, such as Oracle HTTP Server, you must back up the following Windows Registry key:

HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services

Run-time artifacts are those files that change frequently. Back up these files when you perform a full backup and on a regular basis. Run-time artifacts include:

- Domain directories of the Administration Server and the Managed Servers.
In most cases, you do not need to back up Managed Server directories separately because the Administration Server contains information about all of the Managed Servers in its domain.
- Application artifacts, such as *.ear* or *.war* files that reside outside of the domain.
You do not need to back up application artifacts in a Managed Server directory structure because they can be retrieved from the Administration Server during Managed Server startup.
- Any database-based metadata repositories used by Oracle Fusion Middleware.
- Persistent stores, such as JMS Providers and transaction logs.

17.1.3 Recommended Backup Strategy

This section outlines the recommended strategy for performing backups. Using this strategy ensures that you can perform the recovery procedures in this book.

- **Perform a full offline backup:** This involves backing up the entities described in [Section 17.1.2](#). Perform a full offline backup at the following times:

- Immediately after you install Oracle Fusion Middleware
- Immediately before patching or upgrading your Oracle Fusion Middleware environment
- Immediately before an operating system upgrade
- Immediately after upgrading or patching Oracle Fusion Middleware

See [Section 17.3.1](#) for information on performing a full backup.

- **Perform an online backup of run-time artifacts:** This involves backing up the run-time artifacts described in [Section 17.1.2](#). Backing up the run-time artifacts enables you to restore your environment to a consistent state as of the time of your most recent configuration and metadata backup. To avoid an inconsistent backup, do not make any configuration changes until backup completes. Perform an online backup of run-time artifacts at the following times:
 - After every administrative change and on a regular basis. Oracle recommends that you back up run-time artifacts nightly.
 - Prior to making configuration changes to a component.
 - After making configuration changes to a component.
 - Prior to deploying a custom Java EE application to a Managed Server or cluster.
 - After a major change to the deployment architecture, such as creating servers or clusters.

See [Section 17.3.2](#) for information on performing a backup of run-time artifacts.

If you are performing an online backup, do not make any configuration changes until the backup is completed. To ensure that no changes are made in the WebLogic Server domain, lock the WebLogic Server configuration, as described in [Section 2.3.2](#).

- **Perform a new full backup after a major change,** such as any upgrade or patch, or if any of the following files are modified:

```
DOMAIN_HOME/nodemanager/nodemanager.properties
ORACLE_HOME/wlserver/common/bin/wlsifconfig.sh
ORACLE_HOME/wlserver/common/bin/setPatchEnv.sh
ORACLE_HOME/wlserver/common/bin/commEnv.sh
```

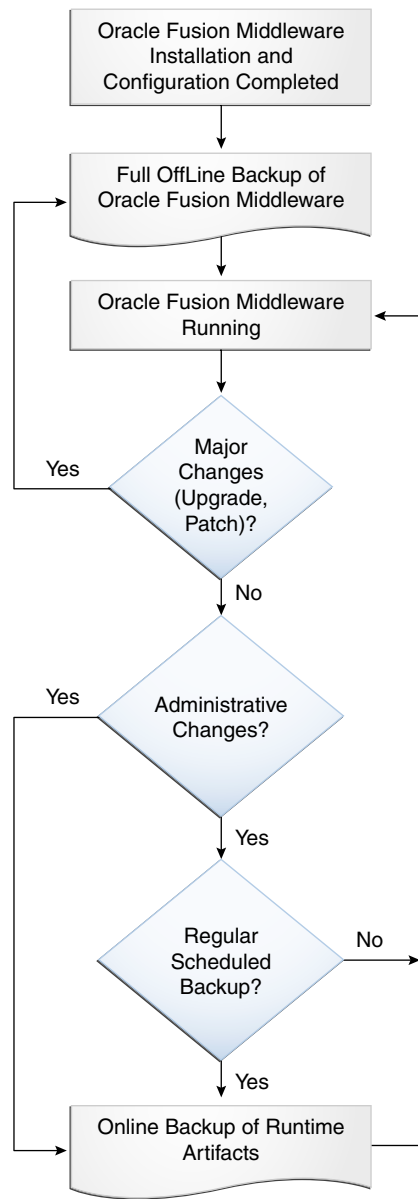
See [Section 17.3.1](#) for information on performing a full backup.

- **Perform a full or incremental backup of your databases:** Use RMAN to backup your databases. See the *Oracle Database Backup and Recovery User's Guide* for information about using RMAN and for suggested methods of backing up the databases.
- Create a record of your Oracle Fusion Middleware environment. See [Section 17.4](#).
- When you create the backup, name the archive file with a unique name. Consider appending the date and time to the name. For example, if you create a backup of the Oracle home on June 5, 2014, name the backup:

```
oracle_home_backup_06052014.tar
```

The flowchart in [Figure 17-1](#) provides an overview of how to decide which type of backup is appropriate for a given circumstance.

Figure 17–1 Decision Flow Chart for Type of Backup



17.2 Limitations and Restrictions for Backing Up Data

Note the following points:

- LDAP backups: If you use the built-in LDAP, do not update the configuration of a security provider while a backup of LDAP data is in progress. If a change is made (for example, if an administrator adds a user), while you are backing up the LDAP directory tree, the backups in the ldapfiles subdirectory could become inconsistent. Refer to *WebLogic Server Managing Server Startup and Shutdown* for detailed LDAP backup procedures.
- Java Transaction API (JTA): Oracle does not recommend that you back up and restore JTA transaction logs.

- **Audit Framework:** If you have configured Oracle Fusion Middleware Audit Framework to write data to a database, you should not back up the local files in the bus stop. (Auditable events from each component are stored in a repository known as a bus stop; each Oracle WebLogic Server has its own bus stop. Data can be persisted in this file, or uploaded to a central repository at which point the records are available for viewing and reporting.)

If you back up the local files, duplicate records are uploaded to the database. That is, they are uploaded to the database when the bus stop is created and then are uploaded again when you restore the files.

The default locations for bus stop local files are:

- For Java components:

`DOMAIN_HOME/servers/server_name/logs/auditlogs/component_type`

- For system components, such as Oracle HTTP Server:

`DOMAIN_HOME/auditlogs/component_type/component_name`

For more information about Oracle Fusion Middleware Audit Framework and the bus stop, see "Configuring and Managing Auditing" in *Securing Applications with Oracle Platform Security Services*.

17.3 Performing a Backup

You can perform a full offline backup or an online or offline backup of run-time artifacts, as described in the following topics:

- [Performing a Full Offline Backup](#)
- [Performing an Online Backup of Run-Time Artifacts](#)
- [Backing Up Windows Registry Entries](#)

17.3.1 Performing a Full Offline Backup

To perform a full offline backup, you copy the directories that contain Oracle Fusion Middleware files.

Archive and compress the source Oracle home, using your preferred tool for archiving, as described in [Section 16.3](#).

Take the following steps:

1. Shut down all processes in the Oracle home. For example, shut down the Managed Servers, the Administration Server, and any system components.
2. Back up the Oracle home (ORACLE_HOME) on all hosts. For example:


```
(UNIX) tar -cf oracle_home_backup_06052014.tar ORACLE_HOME/*
(Windows) jar cMf oracle_home_backup_06052014.jar ORACLE_HOME\*
```
3. Back up the Administration Server domain separately. This backs up Java components and any system components in the domain.

For example:

```
(UNIX) tar -cf domain_home_backup_06052014.tar DOMAIN_HOME/*
(Windows) jar cMf domain_home_backup_06052014.jar DOMAIN_HOME\*
```

In most cases, you do not need to back up the Managed Server directories separately, because the Administration Server domain contains information about the Managed Servers in its domain. If you have customized your environment for the Managed Server, back up the Managed Server directories. See [Section 16.4](#) for information about what you need to back up.

4. If a Managed Server is not located within the domain, back up the Managed Server directory. For example:

```
(UNIX) tar -cf mg1_home_backup_06052014.tar server_name/*
(Windows) jar cMf mg1_home_backup_06052014.jar server_name\*
```

5. Back up the application home directory. For example:

```
(UNIX) tar -cf app_home_backup_06052014.tar Applications_Home/domain_name/*
(Windows) jar cMf app_home_backup_06052014.jar Applications_Home\domain_name\*
```

6. Back up the OraInventory directory. For example:

```
tar -cf Inven_home_backup_06052014.tar /scratch/oracle/OraInventory
```

7. On Linux and UNIX, back up the oraInst.loc file, which is located in the following directory:

```
(Linux and IBM AIX) /etc
(Other UNIX systems) /var/opt/oracle
```

8. On Linux and UNIX, backup the oratab file, which is located in the following directory:

```
/etc
```

9. Back up the database repositories using the Oracle Recovery Manager (RMAN). For detailed steps, see the *Oracle Database Backup and Recovery User's Guide*.
10. On Windows, export the Windows Registry entries, as described in [Section 17.3.3](#).
11. Unlock the WebLogic Server configuration by clicking Release Configuration on the WebLogic Server Administration Console,
12. Create a record of your Oracle Fusion Middleware environment. See [Section 17.4](#).

17.3.2 Performing an Online Backup of Run-Time Artifacts

You should perform a backup of run-time artifacts (which are listed in [Section 17.1.2](#)) on a regular basis and at the times described in [Section 17.1.3](#).

To back up run-time artifacts:

1. To avoid an inconsistent backup, do not make any configuration changes until the backup is completed. To ensure that no changes are made in the WebLogic Server domain, lock the WebLogic Server configuration, as described in [Section 2.3.2](#).

2. Back up the Administration Server domain directories. For example:

```
UNIX) tar -cf domain_home_backup_06052014.tar DOMAIN_HOME/*
(Windows) xcopy c:\DOMAIN_HOME e:\domain_home_backup_06052014 /s /e /i /h
```

3. Back up the application home directory. For example:

```
(UNIX) tar -cf app_home_backup_06052014.tar DOMAIN_HOME/*
(Windows) jar cMf app_home_backup_06052014.jar C:\oracle\applications\domain_name\*
```

4. Back up the database repositories using the Oracle Recovery Manager (RMAN). For detailed steps, see the *Oracle Database Backup and Recovery User's Guide*.
5. Unlock the Oracle WebLogic Server configuration by clicking **Release Configuration** on the WebLogic Server Administration Console,
6. Create a record of your Oracle Fusion Middleware environment. See [Section 17.4](#).

17.3.3 Backing Up Windows Registry Entries

On Windows, you must back up Windows Registry keys related to Oracle Fusion Middleware. Which keys you back up depends on what components you have installed.

To export a key, use the following command:

```
regedit /E FileName Key
```

Export the following entries:

- For any component, export the following registry key:

```
HKEY_LOCAL_MACHINE\Software\Oracle
```

- For system components, such as Oracle HTTP Server, export each node that begins **Oracle** within the following registry keys:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
```

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services
```

```
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services
```

For example:

```
regedit /E C:\oracleSMP.reg HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services
```

Use a unique file name for the each key.

You can also use the Registry Editor to export the key. See the Registry Editor Help for more information.

17.4 Creating a Record of Your Oracle Fusion Middleware Configuration

In the event that you need to restore and recover your Oracle Fusion Middleware environment, it is important to have all the necessary information at your disposal. This is especially true in the event of a hardware loss that requires you to reconstruct all or part of your Oracle Fusion Middleware environment on a new disk or host.

You should maintain an up-to-date record of your Oracle Fusion Middleware environment that includes the information listed in this section. You should keep this information both in hardcopy and electronic form. The electronic form should be stored on a host or e-mail system that is completely separate from your Oracle Fusion Middleware environment.

Your Oracle Fusion Middleware hardware and software configuration record should include:

- The following information for each host in your environment:
 - Host name
 - Virtual host name (if any)
 - Domain name

- IP address
- Hardware platform
- Operating system release level and patch information
- The version of the JDK and its path used in the installation and configuration of Oracle Fusion Middleware
- The following information for each Oracle Fusion Middleware installation in your environment:
 - Installation type (for example, Oracle HTTP Server)
 - Host on which the installation resides
 - User name, userid number, group name, groupid number, environment profile, and type of shell for the operating system user that owns the Oracle home (/etc/passwd and /etc/group entries)
 - Directory structure, mount points, and full path for the Oracle home, Oracle Common home, product homes, Oracle WebLogic Server domain home (if it does not reside in the user_projects directory in the Oracle home)
 - Amount of disk space used by the installation
 - Port numbers used by the installation
 - The version of the JDK and its path used in the installation and configuration of Oracle Fusion Middleware
- The following information for the database containing the metadata for components:
 - Host name
 - Database version and patch level
 - Base language
 - Character set
 - Global database name
 - SID
 - Listen port

Recovering Your Environment

This chapter describes recommended recovery strategies and procedures for recovering Oracle Fusion Middleware from different types of failures and outages, such as media failures or loss of host.

This chapter includes the following sections:

- [Section 18.1, "Overview of Recovery Strategies"](#)
- [Section 18.2, "Recovering After Data Loss, Corruption, Media Failure, or Application Malfunction"](#)
- [Section 18.3, "Recovering After Loss of Host"](#)

18.1 Overview of Recovery Strategies

Recovery strategies enable you to recover from critical failures that involve actual data loss. Depending on the type of loss, they can involve recovering any combination of the following types of files:

- Oracle software files
- Configuration files
- Oracle system files
- Windows Registry keys
- Application artifacts

You can recover your Oracle Fusion Middleware environment while Oracle Fusion Middleware is offline.

The following topics describe recovery strategies:

- [Types of Recovery](#)
- [Recommended Recovery Strategies](#)

18.1.1 Types of Recovery

You can recover your Oracle Fusion Middleware environment in part or in full. You can recover the following:

- The Oracle home
- WebLogic Server domains
- Standalone domains
- The Administration Server

- Managed Servers
- A component, such as Oracle SOA Suite or Oracle HTTP Server
- WebLogic Server cluster
- Deployed applications
- The database

18.1.2 Recommended Recovery Strategies

This section provides an overview of recovery strategies for outages that involve actual data loss or corruption, host failure, or media failure where the host or disk cannot be restarted and they are permanently lost. This type of failure requires some type of data restoration before the Oracle Fusion Middleware environment can be restarted and continue with normal processing.

Note: The procedures in this chapter assume that no administrative changes were made since the last backup. If administrative changes were made since the last backup, they must be reapplied after recovery is complete.

Note the following key points about recovery:

- Your Oracle Fusion Middleware environment must be offline while you are performing recovery.
- Rename important existing files and directories before you begin restoring the files from backup so that you do not unintentionally override necessary files.
- Although, in some cases, it may appear that only one or two files are lost or corrupted, you should restore the directory structure for the entire element, such as a domain, rather than just restoring one or two files. In this way, you are more likely to guarantee a successful recovery.
- Recover the database to the most current state, using point-in-time recovery (if the database is configured in Archive Log Mode). This is typically a time right before the database failure occurred.
- When you restore the files, use your preferred tool to extract the compressed files, as described in [Section 16.3](#).

Ensure that the tool you are using preserves the permissions and timestamps of the files.

When you recover your environment, it is important to recover the entities in the correct order:

1. The database, if it needs to be recovered. See [Section 18.2.9](#) and [Section 18.3.7](#).
2. The Oracle Home, if it needs to be recovered. See [Section 18.2.1](#).
3. The entire domain, if it needs to be recovered. See [Section 18.2.2](#) and [Section 18.3.1](#) for recovering a WebLogic Server managed domain. See [Section 18.2.3](#) for recovering a standalone domain.
4. The Administration Server, if you do not need to recover the domain. See [Section 18.2.4](#) and [Section 18.3.3](#).
5. The Managed Servers, if they are not in the Administration Server domain directory and they need to be recovered. See [Section 18.2.5](#) and [Section 18.3.4](#).

Java components are recovered when you recover the Managed Server. System components are recovered when you recover the domain. In some circumstances, you may need to take certain steps as described in [Section 18.2.6](#) and [Section 18.3.5](#).

Some components require additional actions, which are described in the sections listed in [Table 18–1](#).

Table 18–1 Additional Recovery Procedures for Particular Components

Component	For Data Loss, Corruption, Media Failure	For Loss of Host
Oracle B2B	Section 18.2.6.2	Section 18.2.6.2
Oracle Data Integrator	NA	Section 18.3.5.6
Oracle HTTP Server	NA	Section 18.3.5.5
Oracle Platform Security Services	Section 18.2.6.1	Section 18.2.6.1
Oracle SOA Suite	NA	No additional steps needed if recovering to the same host. For recovering to a different host, Section 18.3.5.4 .
Oracle WebLogic Server	For Oracle WebLogic Server with whole server migration, see Section 18.2.2.1 .	For Oracle WebLogic Server with whole server migration, see Section 18.2.2.1 .

6. Applications, if they need to be recovered. See [Section 18.2.8](#).

18.2 Recovering After Data Loss, Corruption, Media Failure, or Application Malfunction

This section describes recovery strategies for outages that involve actual data loss or corruption, or media failure where the disk cannot be restored. It also describes recovery strategies for applications that are no longer functioning properly. This type of failure requires some type of data restoration before the Oracle Fusion Middleware environment can be restarted and continue with normal processing. It contains the following topics:

- [Recovering the Oracle Home](#)
- [Recovering an Oracle WebLogic Server Domain](#)
- [Recovering a Standalone Domain](#)
- [Recovering the Administration Server Configuration](#)
- [Recovering a Managed Server](#)
- [Recovering a Component](#)
- [Recovering a Cluster](#)
- [Recovering Applications](#)
- [Recovering a Database](#)

Note: You can only restore an entity to the same path as the original entity. That path can be on the same host or a different host.

18.2.1 Recovering the Oracle Home

You can recover the Oracle home that was corrupted or from which files were deleted.

To recover the Oracle home:

1. Stop all relevant processes. That is, stop all processes that are related to the domain, such as the Administration Server, Node Manager, and Managed Servers. For example, to stop the Administration Server on Linux:

```
DOMAIN_HOME/bin/stopWebLogic.sh username password [admin_url]
```

2. Change to the directory that you want to be the parent directory of the Oracle home directory. Use the same directory structure as in the original environment.
3. Recover the Oracle home directory from backup. For example:

```
(UNIX) tar -xf oracle_home_backup_06052014.tar  
(Windows) jar xf oracle_home_backup_06052014.jar
```

4. Start all relevant processes. That is, start all processes that run in the Oracle home, such as the Administration Server and Managed Servers. For example, start the Administration Server:

```
DOMAIN_HOME/bin/startWebLogic.sh
```

18.2.2 Recovering an Oracle WebLogic Server Domain

You can recover an Oracle WebLogic Server domain that was corrupted or deleted from the file system, or when the host containing the domain was lost.

Caution: Performing a domain-level recovery can impact other aspects of a running system and all of the configuration changes performed after the backup was taken will be lost.

To recover an Oracle WebLogic Server domain that was corrupted or deleted from the file system:

1. If any relevant processes are running, stop them. That is, stop all processes that are related to the domain, such as the Administration Server, Managed Servers, and any system components. For example, stop the Administration Server:

```
DOMAIN_HOME/bin/stopWebLogic.sh username password [admin_url]
```

For information on stopping system components such as Oracle HTTP Server, see [Section 4.3.2](#).

2. Change to the directory that you want to be the parent directory of the domain home directory. Use the same directory structure as in the original environment.
3. Recover the domain directory from backup:

```
(UNIX) tar -xf domain_backup_06052014.tar  
(Windows) jar xf domain_backup_06052014.jar
```

4. Start all relevant processes. That is, start all processes that are related to the domain, such as the Administration Server, Managed Servers, and any system components. For example, start the Administration Server:

```
DOMAIN_HOME/bin/startWebLogic.sh
```

For information on starting system components such as Oracle HTTP Server, see [Section 4.3.2](#).

5. If you cannot start the Administration Server, recover it, as described in [Section 18.2.4](#).
6. If you cannot start a Managed Server, recover it, as described in [Section 18.2.5](#).

18.2.2.1 Recovering Oracle WebLogic Server with Whole Server Migration

When using database leasing (for example, with whole server migration), if you recover Oracle WebLogic Server, you should discard the information in the leasing table. You can simply drop and recreate the leasing table by running the leasing table creation script. (For more information about Whole Server Migration, see "Whole Server Migration" in *Administering Clusters for Oracle WebLogic Server*.)

18.2.3 Recovering a Standalone Domain

You can recover a standalone domain that contains system components, such as Oracle HTTP Server, that was corrupted or deleted from the file system or if the host was lost and you want to recover to the same host.

To recover a standalone domain:

1. If Node Manager or a system component, such as Oracle HTTP Server are running, stop them.
2. If it is corrupted, recover the Oracle home:

```
(UNIX) tar xf oracle_home_backup_05_21_2013.tar
(Windows) jar xf oracle_home_backup_05_21_2013.jar
```

3. Recover the domain home:

```
(UNIX) tar xf domain_backup_05_21_2013.tar
(Windows) jar xf domain_backup_05_21_2013.jar
```

4. Start Node Manager:

```
(UNIX) DOMAIN_HOME/bin/startNodeManager.sh
(Windows) DOMAIN_HOME\bin\startNodeManager.cmd
```

5. Start any system components, such as Oracle HTTP Server, that are in the domain:

```
(UNIX) Domain_Home/bin/startComponent.sh ohs1
(Windows) Domain_Home\bin\startComponent.cmd ohs1
```

18.2.4 Recovering the Administration Server Configuration

If the Administration Server configuration has been lost because of file deletion or file system corruption, the Administration Server console continues to function if it was already started when the problem occurred. To prevent the Administration Server from prompting for a user name and password, see [Section 4.2.4](#).

Caution: Performing a domain-level recovery can impact other aspects of a running system and all of the configuration changes performed after the backup was taken will be lost.

To recover the Administration Server configuration:

1. Stop all processes, including the Administration Server, Managed Servers, and Node Manager, if they are started. For example, to stop the Administration Server:

```
DOMAIN_HOME/bin/stopWebLogic.sh username password [admin_url]
```

2. Recover the Administration Server configuration by recovering the domain home backup to a temporary location. Then, restore the config directory to the following location:

```
DOMAIN_HOME/config
```

3. Start the Administration Server. For example:

```
DOMAIN_HOME/bin/startWebLogic.sh
```

4. Verify that the Administration Server starts properly and is accessible.

On the next configuration change, the configuration from the Administration Server is pushed to the Managed Servers. On each Managed Server restart, the configuration is retrieved from the Administration Server.

18.2.5 Recovering a Managed Server

You can recover a Managed Server's files, including its configuration files if they are deleted or corrupted.

In this scenario, the Managed Server is not on the same host as the Administration Server, and it does not operate properly or cannot be started because the configuration has been deleted or corrupted or the configuration was mistakenly changed and you cannot ascertain what was changed.

To recover a Managed Server:

1. If the Administration Server is not reachable, recover the Administration Server, as described in [Section 18.2.4](#).

2. If the Managed Server is running, stop it. For example:

```
DOMAIN_HOME/bin/stopManagedWeblogic.sh managed_server_name admin_url  
username password
```

3. Recover the Oracle home from the backup, if required. For example:

```
tar -xf oracle_home_backup_06052014.tar
```

4. Stop Node Manager as described in [Section 4.2.2](#).

5. Create a domain template jar file for the Administration Server, using the pack utility on the Administration Server host. For example:

```
pack.sh -domain=/scratch/oracle/config/domains/WLS_domain  
-template=/scratch/temp.jar -template_name=test_install  
-template_author=myname -log=/scratch/logs/my.log -managed=true
```

Specifying the `-managed=true` option packs up only the Managed Servers. If you want to pack the entire domain, omit this option.

6. Unpack the domain template jar file, using the `unpack` utility on the Managed Server host. In the following example, `temp.jar` is the archive created by the `pack` command:

```
unpack.sh -template=/scratch/temp.jar
-domain=/scratch/oracle/config/domains/WLS_domain
-log=/scratch/logs/new.log -log_priority=info
```

Note:

- The following directory must exist. If it does not the `unpack` command fails.

ORACLE_HOME/config/domains/

- The `unpack` command provides an `-overwrite_domain` option, which allows unpacking a Managed Server template into an existing domain and existing applications directories. For any file that is overwritten, a backup copy of the original is created. Use the `-overwrite_domain` option, if required for your deployment.
- By default, applications are stored in the following directory unless you pass another location using the `-app_dir` argument:

ORACLE_HOME/user_projects/applications/Domain_Name

7. Start the Managed Server. For example:

```
DOMAIN_HOME/bin/startManagedWebLogic.sh managed_server_name admin_url
```

The Managed Server connects to the Administration Server and updates its configuration changes.

18.2.6 Recovering a Component

You can recover a component if the component's files have been deleted or corrupted or if the component cannot be started or is not functioning properly because the component's configuration was changed and committed. You may not be able to ascertain what change is causing the problem and you want to revert to an earlier version.

- For Java components, you recover the Managed Server, as described in [Section 18.2.5](#).
- For system components, such as Oracle HTTP Server, in a standalone domain, you recover the domain, as described in [Section 18.2.3](#).
- For system components, such as Oracle HTTP Server, in an Oracle WebLogic Server domain, you recover the domain as described in [Section 18.2.2](#).

The following sections describes additional steps you must take for certain components:

- [Recovering Oracle Platform Security Services](#)
- [Recovering Oracle B2B](#)

18.2.6.1 Recovering Oracle Platform Security Services

For Oracle Platform Security Services, restore the following files:

```
DOMAIN_HOME/config/fmwconfig/jps-config.xml
DOMAIN_HOME/config/fmwconfig/jps-config-jse.xml
DOMAIN_HOME/config/fmwconfig/cwallet.sso
DOMAIN_HOME/config/fmwconfig/bootstrap/cwallet.sso
DOMAIN_HOME/config/fmwconfig/keystores.xml
DOMAIN_HOME/config/config.xml
DOMAIN_HOME/config/fmwconfig/ids_config.xml
DOMAIN_HOME/config/fmwconfig/system-jazn-data.xml (if present)
DOMAIN_HOME/config/fmwconfig/jps_mbeans.xml
```

18.2.6.2 Recovering Oracle B2B

After recovery, if the file Xengine.tar.gz is not unzipped, unzip the files. For example:

```
cd B2B_ORACLE_HOME/soa/thirdparty/edifecs
tar xzvf XEngine.tar.gz
```

18.2.7 Recovering a Cluster

You may need to recover a cluster in the following situations:

- The cluster has been erroneously deleted, a cluster member was erroneously deleted.
- The cluster-level configuration, such as the JMS configuration or container-level data sources, was mistakenly changed and committed. The component or server cannot be started or does not operate properly or the services running inside the server are not starting. You may not be able to ascertain what change is causing the problem and you want to revert to an earlier version.

Caution: Performing a domain-level recovery can impact other aspects of a running system and all of the configuration changes performed after the backup was taken will be lost.

If the configuration changes are few, then the easiest way is to redo the configuration changes. If that is not feasible, use the following procedure to recover the configuration:

1. Stop the cluster. You can use the Oracle WebLogic Server Administration Console or WLST. For example, to use WLST:

```
shutdown('cluster_name', 'Cluster')
```

2. Stop all processes, such as the Administration Server and Managed Servers. For example, to stop the Administration Server:

```
DOMAIN_HOME/bin/stopWebLogic.sh username password [admin_url]
```

3. Recover the Administration Server configuration by recovering the domain home backup to a temporary location. Then, restore the config directory to the following location:

```
DOMAIN_HOME/config
```

4. Start the Administration Server. For example:

```
DOMAIN_HOME/bin/startWebLogic.sh
```


Any deleted members are now back in the cluster.

5. Start all processes, such as the Managed Servers. For example, to start the Managed Server on Linux, use the following script:

```
DOMAIN_HOME/bin/startManagedWebLogic.sh managed_server_name admin_url
```

6. Start the cluster. You can use the Oracle WebLogic Server Administration Console or WLST. For example, to use WLST:

```
start('cluster_name', 'Cluster')
```

18.2.8 Recovering Applications

The following topics describe how to recover an application:

- [Recovering Application Artifacts](#)
- [Recovering a Java EE Application](#)

Note the following about recovering applications:

- If the application is staged, the Administration server copies the application bits to the staged directories on the Managed Server hosts.
- If the deployment mode is `nostage` or `external_stage`, ensure that additional application artifacts are available. For example, applications may reside in directories outside of the domain directory. Make your application files available to the new Administration Server by copying them from backups or by using a shared disk. Your application files should be available in the same relative location on the new file system as on the file system of the original Administration Server.

See Also: *Deploying Applications to Oracle WebLogic Server* for information about deploying applications

18.2.8.1 Recovering Application Artifacts

If an application's artifacts, such as the `.ear` file, have been lost or corrupted, you can recover the application.

To recover the application:

1. Start the Managed Server to which the application was deployed. For example:

```
DOMAIN_HOME/bin/startManagedWebLogic.sh managed_server_name admin_url
```

This synchronizes the configuration with the Administration Server.

On each Managed Server restart, the configuration and application artifacts are retrieved from the Administration Server.

18.2.8.2 Recovering a Java EE Application

You can recover a Java EE application:

- If a Java EE application was redeployed to a Managed Server (whether or not the Managed Server is part of a cluster) and the application is no longer functional.
- If a deployed application was undeployed from Oracle WebLogic Server.
- A new version of a composite application was redeployed to a Managed Server or cluster. The application is no longer functional.

To recover the application:

1. Recover the application files from backup, if needed.
2. Redeploy the old version of the application from the backup.

You cannot just copy the original ear file. Even if the original ear file (from the backup) is copied back to the Managed Server stage directory and you restart the Managed Server, the application is still not recovered. You must redeploy the original version.

18.2.9 Recovering a Database

If your database that contains your metadata repository, including the MDS Repository, is corrupted, you can recover it using RMAN. You can recover the database at the desired granularity, either a full recovery or a tablespace recovery.

For best results, recover the database to the most current state, using point-in-time recovery (if the database is configured in Archive Log Mode.) This ensures that the latest data is recovered. For example:

```
rman> restore database;  
rman> recover database;
```

See *Creating Schemas with the Repository Creation Utility* for the schemas used by each component.

For detailed steps, see the *Oracle Database Backup and Recovery User's Guide*.

18.3 Recovering After Loss of Host

This section describes how to recover your Oracle Fusion Middleware environment after losing the original operating environment. For example, you could have a serious system malfunction or loss of media. The sections includes the following topics:

- [Recovering After Loss of Oracle WebLogic Server Domain Host](#)
- [Recovering After Loss of Standalone Domain Host](#)
- [Recovering After Loss of Administration Server Host](#)
- [Recovering After Loss of Managed Server Host](#)
- [Recovering After Loss of Component Host](#)
- [Additional Actions for Recovering Entities After Loss of Host](#)
- [Recovering After Loss of Database Host](#)

Note: When you are recovering in the case of loss of host, you must restore the files using the same path as on the original host.

18.3.1 Recovering After Loss of Oracle WebLogic Server Domain Host

To recover an Oracle WebLogic Server domain after loss of host, follow the steps in [Section 18.2.2](#).

18.3.2 Recovering After Loss of Standalone Domain Host

If you lose a host that contains a standalone domain, you can recover it to the same host or a different host, as described in the following topics:

- [Recovering a Standalone Domain to the Same Host](#)

- [Recovering a Standalone Domain to a Different Host](#)

18.3.2.1 Recovering a Standalone Domain to the Same Host

To recover the standalone domain to the same host after the operating system has been reinstalled, follow the procedures in [Section 18.2.3](#).

18.3.2.2 Recovering a Standalone Domain to a Different Host

In this scenario, you recover the standalone domain to a different host.

To recover the standalone domain to a different host:

1. Recover the Oracle home:

```
(UNIX) tar xf oracle_home_backup_05_21_2014.tar
(Windows) jar xf oracle_home_backup_05_21_2014.jar
```

2. Recover the domain home:

```
(UNIX) tar xf domain_backup_05_21_2014.tar
(Windows) jar xf domain_backup_05_21_2014.jar
```

3. In a standalone domain, by default, Node Manager is listening on localhost. However, if it is not, you can update the ListenAddress by using the following WLST commands:

```
readDomain('Domain_Home')
cd('/')
cd('NMPProperties')
set('ListenAddress','localhost')
set('ListenPort',9001)
```

4. Start Node Manager:

```
(UNIX) DOMAIN_HOME/bin/startNodeManager.sh
(Windows) DOMAIN_HOME\bin\startNodeManager.cmd
```

5. Update any system component configuration files manually.

See [Section 18.3.5](#) for details for specific components.

6. Start any system components, such as Oracle HTTP Server, that are in the domain. For example:

```
(UNIX) Domain_Home/bin/startComponent.sh ohs1
(Windows) Domain_Home\bin\startComponent.cmd ohs1
```

7. Update the Oracle Inventory, as described in [Section 18.3.6.4](#).
8. For Windows, update the Windows Registry, as described in [Section 18.3.6.5](#).

18.3.3 Recovering After Loss of Administration Server Host

If you lose a host that contains the Administration Server, you can recover it to the same host or a different host, as described in the following topics:

- [Recovering the Administration Server to the Same Host](#)
- [Recovering the Administration Server to a Different Host](#)

18.3.3.1 Recovering the Administration Server to the Same Host

In this scenario, you recover the Administration Server either to the same host after the operating system has been reinstalled or to a new host that has the same host name. For example, the Administration Server is running on Host A and the Managed Server is running on Host B. Host A has failed for some reason and the Administration Server must be recovered.

To recover the Administration Server to the same host:

1. Recover the file system. For example, recover the domain containing the Administration Server, as described in [Section 18.3.1](#).
2. Attempt to start the Administration Server. For example:

```
DOMAIN_HOME/bin/startWebLogic.sh
```

If the Administration Server starts, you do not need to take any further steps.

3. If the Administration Server fails to start, take the following steps on Host A:
 - a. Stop all relevant processes. That is, stop all processes that are related to the domain, such as the Managed Servers.
 - b. Recover the Oracle home, if needed:

```
tar -xf oracle_home_backup_06052014.tar
```

- c. If the domain directory does not reside in the Oracle home, recover the domain directory from backup. First, change to the directory that you want to be the parent of the Domain home, then:

```
tar -xf domain_backup_06052014.tar
```

- d. Start the Administration Server. For example:

```
DOMAIN_HOME/bin/startWebLogic.sh
```

- e. Start the Managed Servers, specifying the Administration URL for the host:

```
DOMAIN_HOME/bin/startManagedWebLogic.sh managed_server_name admin_url
```

- f. Start Node Manager:

```
cd DOMAIN_HOME/bin  
./startNodeManager.sh
```

18.3.3.2 Recovering the Administration Server to a Different Host

In this scenario, the Administration Server is running on Host A and the Managed Server is running on Host B. Host A has failed for some reason and the Administration Server must be moved to Host C.

To recover the Administration Server to a different host:

1. Recover the Oracle home to Host C (the new Host):

```
tar -xf oracle_home_backup_06052014.tar
```

2. If the domain directory does not reside in the Oracle home, recover the domain directory from backup. First, change to the directory that you want to be the parent of the Domain home, then:

```
tar -xf domain_backup_06052014.tar
```

3. If the Administration Server has a Listen address, create a new machine with the new host name, as described in [Section 18.3.6.3](#).

4. Start the Administration Server. For example:

```
DOMAIN_HOME/bin/startWebLogic.sh
```

5. Using WLST, connect to the Administration Server and then enroll Node Manager running in the new host with the Administration Server:

```
connect('username', 'password', 't3://host:port')
nmEnroll('/scratch/oracle/config/domains/domain_name',
        'DOMAIN_HOME/nodemanager')
```

Note that on Windows, as on UNIX, you use slashes (/), not backslashes (\), in the nmEnroll command.

6. Edit the Node Manager properties file, changing the Listen Address property. For a domain-based Node Manager, the file is located at:

```
DOMAIN_HOME/nodemanager/nodemanager.properties
```

Alternatively, you can use the following WLST commands to change the property:

```
readDomain('Domain_Home')
cd('/')
cd('NMPProperties')
set('ListenAddress', 'localhost')
set('ListenPort', port_num)
```

7. Start Node Manager on Host C if it was configured on the original host:

```
cd DOMAIN_HOME/bin
./startNodeManager.sh
```

8. Start the Managed Servers. The section "Restarting a Failed Administration Server" in *Administering Server Startup and Shutdown for Oracle WebLogic Server* describes different ways to restart them, depending on how they were configured.

One option is to use the following script, specifying the Administration URL of the new host:

```
DOMAIN_HOME/bin/startManagedWebLogic.sh managed_server_name admin_url
```

9. Ensure that additional application artifacts are available. For example, if the deployment mode is `nostage` or `external_stage`, applications may reside in directories outside of the domain directory. Make your application files available to the new Administration Server by copying them from backups or by using a shared disk. Your application files should be available in the same relative location on the new file system as on the file system of the original Administration Server.

If the application is staged, the Administration Server copies the application bits to the staged directories on the Managed Server hosts.

10. Update Oracle Inventory, as described in [Section 18.3.6.4](#).
11. On Windows, recover the Windows Registry, as described in [Section 18.3.6.5](#)
12. If your environment contains Oracle HTTP Server, modify the `mod_wl_ohs.conf` file, as described in [Section 18.3.6.2](#).

Now you can start and stop the Managed Server on Host B using the Administration Console running on Host C.

If you are recovering the Administration Server for a Web Tier installation, see [Section 18.3.6](#) for information about additional actions you must take.

18.3.4 Recovering After Loss of Managed Server Host

If you lose a host that contains a Managed Server, you can recover it to the same host or a different host, as described in the following topics:

- [Recovering a Managed Server to the Same Host](#)
- [Recovering a Managed Server to a Different Host](#)

18.3.4.1 Recovering a Managed Server to the Same Host

In this scenario, you recover a Managed Server to the same host after the operating system has been reinstalled or to a new host that has the same host name. The Administration Server is running on Host A and the Managed Server is running on Host B. Host B failed for some reason and the Managed Server must be recovered to Host B.

To recover a Managed Server to the same host:

1. Start Node Manager on Host B:

```
cd DOMAIN_HOME/bin
./startNodeManager.sh
```

2. Start the Managed Server. For example:

```
DOMAIN_HOME/bin/startManagedWebLogic.sh managed_server_name admin_url
```

If the Managed Server starts, it connects to the Administration Server and updates its configuration changes. You do not need to take any further steps.

3. If the Managed Server fails to start or if the file system is lost, take the following steps:

- a. Recover the Oracle home to Host B from the backup, if required:

```
tar -xf oracle_home_backup_06052014.tar
```

- b. Stop Node Manager as described in [Section 4.2.2](#).

- c. Create a domain template jar file for the Administration Server running in Host A, using the pack utility. For example:

```
pack.sh -domain=/scratch/oracle/config/domains/domain_name
-template=/scratch/temp.jar -template_name=test_install
-template_author=myname -log=/scratch/logs/my.log -managed=true
```

Specifying the `-managed=true` option packs up only the Managed Servers. If you want to pack the entire domain, omit this option.

- d. Unpack the domain template jar file in Host B, using the unpack utility:

```
unpack.sh -template=/scratch/temp.jar
-domain=/scratch/oracle/config/domains/domain_name
-log=/scratch/logs/new.log -log_priority=info
```

- e. Ensure that the application artifacts are accessible from the Managed Server host. That is, if the application artifacts are not on the same server as the Managed Server, they must be in a location accessible by the Managed Server.

Note:

- For applications that are deployed in nostage and external_stage mode, copy the application artifacts from the Administration Server host directory.
- For applications that are deployed in stage mode, the Administration server copies the application bits to the staged directories on the Managed Server hosts.

See *Deploying Applications to Oracle WebLogic Server* for information about deploying applications.

- f. Update the Node Manager property ListenAddress by using the following WLST commands:

```
readDomain('Domain_Home')
cd('/')
cd('NMPProperties')
set('ListenAddress','localhost')
set('ListenPort',9001)
```

- g. If Node Manager is not started, start it:

```
cd DOMAIN_HOME/bin
./startNodeManager.sh
```

- h. Start the Managed Server. For example:

```
DOMAIN_HOME/bin/startManagedWebLogic.sh managed_server_name admin_url
```

The Managed Server connects to the Administration Server and updates its configuration changes.

18.3.4.2 Recovering a Managed Server to a Different Host

In this scenario, the Administration Server is running on Host A and the Managed Server is running on Host B. Host B failed for some reason and the Managed Server must be recovered to Host C. There are two machines, which are logical representations of the computer that hosts one or more WebLogic Servers, machine_1 on Host A and machine_2 on Host B.

Important: Recover the Oracle home to the same location as the original.

To recover a Managed Server to a different host:

1. Recover the Oracle home for the Managed Server to Host C.

```
tar -xf oracle_home_backup_06052014.tar
```

2. Reconfigure the topology to point to the new host:

- a. To avoid an inconsistent backup, do not make any configuration changes until the backup is completed. To ensure that no changes are made in the WebLogic Server domain, lock the WebLogic Server configuration, as described in [Section 2.3.2](#).

- b. In the WebLogic Server Administration Console, change the configuration of machine_2, to point it to the new host:

From the left pane of the Console, expand **Environment** and then select **Machines**. Select machine_2 and select the Configuration tab. Then select the Node Manager tab. Change the **Listen Address** to the address for Host C. Click **Save**.

If you identify the Listen Address by IP address, you must disable Host Name Verification on the Administration Servers that access Node Manager. For more information and instructions, see "Using Hostname Verification" in *Administering Security for Oracle WebLogic Server*.

- c. Change the Managed Server configuration to point to the new host:

From the left pane of the Console, expand **Environment** and then **Servers**. Then, select the name of the server. Select the **Configuration** tab, then the **General** tab.

Change the **Machine** to machine_2.

Change **Listen Address** to the new host. (If the listening address was set to blank, you do not need to change it.)

Click **Save**, then click **Activate Changes**.

- d. Unlock the Oracle WebLogic Server configuration by clicking **Release Configuration** on the WebLogic Server Administration Console,

3. Take any additional steps needed for components as described in [Table 18–1](#).
4. Stop Node Manager as described in [Section 4.2.2](#).
5. Create a domain template jar file from the Administration Server running in Host A, using the pack utility. For example:

```
pack.sh -domain=/scratch/oracle/config/domains/domain_name
        -template=/scratch/temp.jar -template_name=test_install
        -template_author=myname -log=/scratch/logs/my.log -managed=true
```

Specifying the `-managed=true` option packs up only the Managed Servers. If you want to pack the entire domain, omit this option.

6. Unpack the domain template jar file on Host C, using the unpack utility:

```
unpack.sh -template=/scratch/temp.jar
          -domain=/scratch/oracle/config/domains/domain_name
          -log=/scratch/logs/new.log -log_priority=info
```

7. Ensure that the application artifacts are accessible from the Managed Server host. That is, if the application artifacts are not on the same server as the Managed Server, they must be in a location accessible by the Managed Server.

Note:

- For applications that are deployed in `nostage` and `external_stage` mode, copy the application artifacts from the Administration Server host directory.
- For applications that are deployed in `stage` mode, the Administration server copies the application bits to the staged directories on the Managed Server hosts.

See *Deploying Applications to Oracle WebLogic Server* for information about deploying applications.

8. Update the `ListenAddress` by using the following WLST commands:

```
readDomain('Domain_Home')
cd('/')
cd('NMPProperties')
set('ListenAddress','localhost')
set('ListenPort',9001)
```

9. Start Node Manager on Host C, if it is not started:

```
cd DOMAIN_HOME/bin
./startNodeManager.sh
```

10. Start the Managed Server. For example:

```
DOMAIN_HOME/bin/startManagedWebLogic.sh managed_server_name admin_url
```

The Managed Server connects to the Administration Server and updates its configuration changes.

11. Update Oracle Inventory, as described in [Section 18.3.6.4](#).
12. On Windows, recover the Windows Registry, as described in [Section 18.3.6.5](#)
13. If your environment contains Oracle HTTP Server, modify the `mod_wl_ohs.conf` file, as described in [Section 18.3.6.2](#).

Now you can start and stop the Managed Server on Host C using the Administration Server running on Host A.

18.3.5 Recovering After Loss of Component Host

If you lose a host that contains a component (and its Managed Server, if applicable), you can recover most components to the same host or a different host using the procedures described in the following topics:

- [Recovering a Java Component to the Same or Different Host](#)
- [Recovering a Java Component to a Different Host](#)
- [Recovering a System Component to the Same or Different Host](#)
- [Recovering Oracle SOA Suite After Loss of Host](#)
- [Recovering Web Tier Components to a Different Host](#)
- [Recovering Oracle Data Integrator to a Different Host](#)

Some components require additional actions, which are described in the sections listed in [Table 18-1](#).

18.3.5.1 Recovering a Java Component to the Same or Different Host

To recover a Java component to the same host:

1. Recover the Managed Server, as described in [Section 18.3.4.1](#).
2. If the component requires additional steps, as noted in [Table 18–1](#), take those steps.

18.3.5.2 Recovering a Java Component to a Different Host

To recover a Java component to a different host:

1. Recover the Managed Server, as described in [Section 18.3.4.2](#).
2. If the component requires additional steps, as noted in [Table 18–1](#), take those steps.

18.3.5.3 Recovering a System Component to the Same or Different Host

To recover a system component, such as Oracle HTTP Server, to the same host or a different host:

- For system components, such as Oracle HTTP Server, in a standalone domain, you recover the domain, as described in [Section 18.3.2](#).
- For system components, such as Oracle HTTP Server in an Oracle WebLogic Server domain, you recover the domain, as described in [Section 18.3.1](#).

However, note that some components require additional steps, as noted in [Table 18–1](#).

18.3.5.4 Recovering Oracle SOA Suite After Loss of Host

To recover the Oracle SOA Suite Managed Server to the same host, recover the Managed Server, as described in [Section 18.3.4.1](#).

To recover the Oracle SOA Suite Managed Server to a different host after loss of host:

1. Before you recover, update the WSDL file to point to the new host name and port.
2. Recover the Managed Server, as described in [Section 18.3.4.2](#).
3. After you recover the Oracle SOA Suite Managed Server, take the following actions:
 - If the ant command is used to deploy composites, edit the `deploy-sar.xml` file, which is located in:

```
(UNIX) ORACLE_HOME/bin
(Windows) ORACLE_HOME\bin
```

In the following line, replace the previous host name with the new host name:

```
<property name="wlsHost" value="newhostname"/>
```

If a Load Balancer is used, do not modify this property. Instead, register the new host with the Load Balancer.

- Change the host name in the `soa-infra` MBean:
 - a. In Fusion Middleware Control, navigate to the Managed Server.
 - b. From the WebLogic Server menu, choose **System MBean Browser**.
 - c. Expand **Application Defined MBeans**, then `oracle.as.soainfra.config`, then **Server: *server_name*** and then **SoaInfraConfig**. Select **soa-infra**.
 - d. In the Attributes tab, click **ServerURL**. If the ServerURL attribute contains a value, change the host name to the new host name.

e. Click **Apply.**

- Redeploy all applications which have the WSDL files updated to the new host name.

Note: If there is no Load Balancer configured with the environment and Oracle SOA Suite must be recovered to a different host, then in-flight instances that are pending a response from task flow and asynchronous responses are not recovered. Oracle recommends that you use a Load Balancer to ensure that you can recover to a different host.

If a Load Balancer is configured with the environment, take the following additional steps:

1. Log in to the Oracle WebLogic Server Administration Console.
2. In Domain Structure, navigate to Servers. For each Managed Server, select the Protocol tab, then the HTTP tab.
3. For **Frontend Host**, enter the new host name.
4. For **Frontend HTTP Port** and **Frontend HTTPs Port**, if applicable, enter the new port number.
5. Restart each Managed Server.

18.3.5.5 Recovering Web Tier Components to a Different Host

The Web tier consists of Oracle HTTP Server. The following topics describe how to recover it to a different host:

- [Recovering Oracle HTTP Server in a Standalone Domain to a Different Host](#)
- [Recovering Oracle HTTP Server in a WebLogic Server Domain to a Different Host](#)

18.3.5.5.1 Recovering Oracle HTTP Server in a Standalone Domain to a Different Host

To recover Oracle HTTP Server in a standalone domain:

1. Follow steps 1 through 4 in [Section 18.3.2](#).
2. Update the configuration files in the following directory:

```
(UNIX) DOMAIN_HOME/config/fmwconfig/components/OHS/instance_name
(Windows) DOMAIN_HOME\config\fmwconfig\components\OHS\instance_name
```

For example, update the IP Address and host name in `httpd.conf`, `admin.conf`, and `mod_wl_ohs.conf` (if required).

3. Follow steps 6 through 8 in [Section 18.3.2](#).

18.3.5.5.2 Recovering Oracle HTTP Server in a WebLogic Server Domain to a Different Host To recover Oracle HTTP Server in an Oracle WebLogic Server domain to a different host:

1. Recover the domain, as described in [Section 18.3.1](#).
2. Change the configuration of the Oracle HTTP Server instance that was on Host B:
 - a. In Fusion Middleware Control, from the navigation pane, expand **HTTP Server**.
 - b. Select the Oracle HTTP Server instance, such as `ohs1`.

- c. From the Oracle HTTP Server menu, select **Administration**, then **Ports Configuration**.
 - d. For each port in the table, select the port, then click **Edit**. Change the **IP Address**.
Note that if ANY is selected, you do not need to make any changes.
 - e. Click **OK**.
3. Update the mod_wl_ohs wiring for each Oracle HTTP Server instance:
 - a. In Fusion Middleware Control, from the navigation pane, expand **HTTP Server**.
 - b. Select the Oracle HTTP Server instance, such as ohs1.
 - c. From the Oracle HTTP Server menu, select **Administration**, then **mod_wl_ohs Configuration**.
 - d. In the Locations section, click **AutoFill**.
All valid WebLogic Server endpoint locations are displayed.
 - e. Click **Apply**.
 4. Restart any Oracle HTTP Server instances that are not on the failed machine by navigating to that instance and clicking **Start Up**.
 5. Start the Oracle HTTP Server instances on Host C by navigating to that instance and clicking **Start Up**.

18.3.5.6 Recovering Oracle Data Integrator to a Different Host

To recover Oracle Data Integrator, follow the procedures in one or both of these topics, depending on the failure:

- [Recovering Oracle Data Integrator Repository](#)
- [Recovering Oracle Data Integrator Agents to a Different Host](#)

18.3.5.6.1 Recovering Oracle Data Integrator Repository If the Oracle Data Integrator Repository must be restored to a different host:

1. Restore the database, as described in [Section 18.3.7](#).
2. Connect to the restored Oracle Data Integrator repository using ODI Studio. Create a new connection for the master repository to the new database host, as described in "Connecting to the Master Repository" in *Developing Integration Projects with Oracle Data Integrator*.
3. Edit each of the Work Repositories. Click **Connection** and edit the connection information so that the JDBC URL points to the new database host containing the work repository.
4. For the Oracle Data Integrator JEE Agent repository configuration, in the Oracle WebLogic Server configuration, edit the data sources to match the new database host location.
5. Update the Oracle Data Integrator Standalone Agent Repository configuration using the following WLST offline commands:

```
cd ORACLE_HOME/odi/common/bin
./wlst.sh
readDomain('DOMAIN_DIRECTORY')
cd('/JdbcSystemResource/OdiMasterRepository/JdbcResource/OdiMasterRepository/JD
```

```
BCDriverParams/NO_NAME_0');
set('URL', 'NEW_JDBC_URL_TO_RECOVERED_DB');
updateDomain();
exit();
```

18.3.5.6.2 Recovering Oracle Data Integrator Agents to a Different Host To recover Oracle Data Integrator agents to a different host:

1. Restore Oracle Data Integrator JEE Agent by restoring the Managed Server, as described in [Section 18.3.4](#).
2. Restore the Oracle Data Integrator Standalone system component, as described in [Section 18.3.5](#)
3. Use ODI Studio to edit each physical agent's configuration and provide the updated Host Name value and, if changed, the Port value.
4. Update Oracle Data Integrator Standalone Agent's host and port configuration using the following commands:

```
cd ORACLE_HOME/odi/common/bin
./wlst.sh
readDomain('DOMAIN_HOME')
cd('ODI/ODI_STANDALONE_AGENT_NAME')
set("ServerListenAddress", 'UPDATED_HOST_NAME');
set("ServerListenPort", 'UPDATED_PORT');
updateDomain();
exit();
```

5. Restart the standalone agents and the Oracle Data Integrator applications deployed in Oracle WebLogic Server.

18.3.6 Additional Actions for Recovering Entities After Loss of Host

Depending on the entity that you are recovering, you may need to take additional actions after loss of host. The sections about each entity may require you to follow one or more of the following procedures. If so, that is noted in the section describing how to recover the entity.

The following topics describe the actions you may need to take:

- [Recovering Fusion Middleware Control to a Different Host](#)
- [Modifying the mod_wl_ohs.conf File](#)
- [Creating a New Machine for Certain Components](#)
- [Updating Oracle Inventory](#)
- [Recovering the Windows Registry](#)

18.3.6.1 Recovering Fusion Middleware Control to a Different Host

To recover Fusion Middleware Control to a different host, update properties using the System MBean Browser:

1. In Fusion Middleware Control, from the WebLogic Domain menu, select **System MBean Browser**.
2. In the System MBean Browser pane, expand **Application-Defined MBeans**, then **emoms.props**, then **Server: AdminServer**, then **Application: em**, and then **Properties**.
3. Click **emoms.properties**.

4. In the Attributes pane, select the Operations tab and click **setProperty**.
5. Change the value of the following properties to the new host name:
 - oracle.sysman.emSDK.svlt.ConsoleServerHost
 - oracle.sysman.emSDK.svlt.ConsoleServerName

For example, for Key, enter oracle.sysman.emSDK.svlt.ConsoleServerHost. Then, for value, enter host.example.com:7001_Management_Service.

6. Click **Invoke**.

18.3.6.2 Modifying the mod_wl_ohs.conf File

When you recover an Administration Server or a Managed Server to a different host and your environment includes Oracle HTTP Server, you must modify the following file on the new host:

```
(UNIX) DOMAIN_HOME/config/fmwconfig/components/OHS/ohs_name/mod_wl_ohs.conf
(Windows) DOMAIN_HOME\config\fmwconfig\components\OHS\ohs_name\mod_wl_ohs.conf
```

Note that with Oracle HTTP Server in a WebLogic Server domain, this directory is in the Domain home of the Administration Server. With Oracle HTTP Server in a standalone domain, this directory is the Domain home of Oracle HTTP Server.

Modify all of the instances of the host name, port, and clusters (elements such as WebLogicHost, WebLogicPort, and WebLogicCluster) entries in that file. For example:

```
<Location /console>
  SetHandler weblogic-handler
  WebLogicHost Admin_Host
  WebLogicPort Admin_Port
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>
.
.
.
<Location /soa-infra>
  SetHandler weblogic-handler
  WebLogicCluster SOAHOST1VHN2:8001,*SOAHOST2VHN1*:*8001*
  WLProxySSL ON
  WLProxySSLPassThrough ON
</Location>
```

18.3.6.3 Creating a New Machine for Certain Components

If the Administration Server has a Listen address, you must create a new machine with the new host name before you start the Administration Server:

Take the following steps:

1. Create a new machine with the new host name. Use the following WLST commands, in offline mode:

```
wls:/offline> readDomain('DOMAIN_HOME')
wls:/offline/sampledmain> machine = create('newhostname', 'Machine')
wls:/offline/sampledmain> cd('/Machine/newhostname')
wls:/offline/sampledmain> nm = create('newhostname', 'NodeManager')
wls:/offline/sampledmain> cd('/Machine/newhostname/NodeManager/newhostname')
wls:/offline/sampledmain> set('ListenAddress', 'newhostname')
wls:/offline/sampledmain> updateDomain()
wls:/offline/sampledmain> exit()
```

2. For the Administration Server, set the machine with the new host name, using the following WLST command, in offline mode:

```
wls:/offline> readDomain('DOMAIN_HOME')
wls:/offline/sampledomain> cd ('/Machine/newhostname')
wls:/offline/sampledomain> machine = cmo
wls:/offline/sampledomain> cd ('/Server/AdminServer')
wls:/offline/sampledomain> set('Machine', machine)
wls:/offline/sampledomain> updateDomain()
wls:/offline/sampledomain> exit()
```

3. Set the listen port for the Administration Server, using WLST:

```
wls:/offline/sampledomain> readDomain('DOMAIN_HOME')
wls:/offline/sampledomain> cd('/Server/AdminServer')
wls:/offline/sampledomain> cmo.setListenPort(8001)
wls:/offline/sampledomain> updateDomain()
wls:/offline/sampledomain> exit()
```

4. If required, update the Administration Server listen address, using WLST:

```
readDomain('DOMAIN_HOME')
cd('/Server/AdminServer')
cmo.getListenAddress()
cmo.setListenAddress('newhostname')
updateDomain()
exit()
```

18.3.6.4 Updating Oracle Inventory

For many components, when you recover to a different host, as in the case of loss of host, you must update the Oracle inventory. To do so, execute the following script:

```
(UNIX) ORACLE_HOME/oui/bin/attachHome.sh
(Windows) ORACLE_HOME\oui\bin\attachHome.cmd
```

18.3.6.5 Recovering the Windows Registry

When you recover any component to a different host on Windows, as in the case of loss of host, you must import any Windows Registry keys related to Oracle Fusion Middleware to the new host. (You exported the Registry keys in [Section 17.3.3](#).)

Recover the following Registry key.

```
HKEY_LOCAL_MACHINE\Software\Oracle
```

In addition, recover each node that begins with **Oracle** within the following registry keys:

```
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet001\Services
HKEY_LOCAL_MACHINE\SYSTEM\ControlSet002\Services
```

To import a key that you have previously exported, use the following command:

```
regedit /I FileName
```

For example:

```
regedit /I C:\oracleregistry.reg
```

You can also use the Registry Editor to import the key. See the Registry Editor Help for more information.

18.3.7 Recovering After Loss of Database Host

For information about recovering your database, see [Section 18.2.9](#).

Part VIII

Advanced Administration: Expanding Your Environment

This part describes how to expand your Oracle Fusion Middleware environment.

It contains the following chapters:

- [Chapter 19, "Scaling Up Your Environment"](#)
- [Chapter 20, "Moving from a Test to a Production Environment"](#)

Scaling Up Your Environment

You can expand your environment by adding Managed Servers, expanding your domain to include other products, creating a cluster of Managed Servers, creating a standalone domain or system component, and copying existing Oracle homes or domains, as described by the following sections:

- [Section 19.1, "Overview of Scaling Up Your Environment"](#)
- [Section 19.2, "Extending a Domain to Support Additional Components"](#)
- [Section 19.3, "Adding Additional Managed Servers to a Domain"](#)
- [Section 19.4, "Creating Clusters"](#)
- [Section 19.5, "Creating a Standalone Domain and a System Component"](#)
- [Section 19.6, "Creating a System Component Instance in a WebLogic Server Domain"](#)
- [Section 19.7, "Copying an Oracle Home or Component"](#)

19.1 Overview of Scaling Up Your Environment

Scalability is the ability of a system to provide throughput in proportion to, and limited only by, available hardware resources. A scalable system is one that can handle increasing numbers of requests without adversely affecting response time and throughput.

The growth of computational power within one operating environment is called vertical scaling. Horizontal scaling is leveraging multiple systems to work together on a common problem in parallel.

Oracle Fusion Middleware scales both vertically and horizontally.

Oracle Fusion Middleware provides great vertical scalability, allowing you to add more Managed Servers or components to the same host. This is known as scale up.

Horizontally, Oracle Fusion Middleware can provide failover capabilities to another host computer. That way, if one computer goes down, your environment can continue to serve the consumers of your deployed applications. This is also known as scaling out or machine scale out. For information about scaling out, see "Scaling Out a Topology" in the *High Availability Guide*.

Deploying a high availability system minimizes the time when the system is down (unavailable) and maximizes the time when it is running (available). Oracle Fusion Middleware is designed to provide a wide variety of high availability solutions, ranging from load balancing and basic clustering to providing maximum system availability during catastrophic hardware and software failures.

High availability solutions can be divided into two basic categories: local high availability and disaster recovery.

See Also:

- *High Availability Guide* for more information about high availability
- *Disaster Recovery Guide*

19.2 Extending a Domain to Support Additional Components

When you create an Oracle WebLogic Server domain, you create it using a particular domain template. That template supports a particular component or group of components, such as Oracle WebLogic Server. If you want to add other components, such as Oracle HTTP Server, to that domain, you can extend the domain by creating additional Managed Servers in the domain, using a domain template for the component which you want to add.

When you extend a domain, the domain must be offline.

To extend a domain, you use the Oracle WebLogic Server Configuration Wizard from an Oracle home into which the desired component has been installed. Then, you select the domain that you want to extend and the component you want to add. For detailed information, see "Configuring Your WebLogic Domain" in *Installing and Configuring the Oracle Fusion Middleware Infrastructure*.

For example, to extend a domain that initially was created to support Oracle Application Development Framework so that it can now also support Oracle HTTP Server:

1. Use RCU to add any required schemas for the component, as described in *Creating Schemas with the Repository Creation Utility*.
2. Install Oracle HTTP Server, as described in *Installing and Configuring Oracle HTTP Server*.
3. From the Oracle home, invoke the Configuration Wizard, using the following command:

```
(UNIX) ORACLE_HOME/oracle_common/common/bin/config.sh
(Windows) ORACLE_HOME\oracle_common\common\bin\config.cmd
```

The Configuration Wizard's Welcome screen is displayed.

4. Select **Update an existing domain**.
5. In Domain Location, specify the location of the domain.
6. Click **Next**.
7. Select **Update Domain Using Product Templates**.
8. Select **Oracle HTTP Server (colocated)**.
9. Click **Next**.
10. Select **Extend my domain automatically to support the following added products**, Then, select the source from which this domain is to be extended. For example, select **Oracle HTTP Server**.
11. Click **Next**.

12. Select either **RCU Data** or **Manual Configuration**. If you select RCU Data, the information is automatically populated. If you select Manual Configuration, click **Next**.

Select the schemas for the new component you added, entering the following information:

- For **Vendor**, select **Oracle**.
- For **Driver**, select **Oracle's Driver (Thin) for Service connections; Versions:9.0.1,9.2.0,10,11**.
- For **Schema Owner**, do not enter anything. Each data source uses the user name specified in the table.
- If you used the same password when you created the schemas, select all of the schemas and enter the password in **Schema Password**.

Alternatively, you can specify different passwords for each data source by selecting each schema individually and entering the password.

- With all of the schemas selected, for **DBMS/Service**, enter the SID of the database.
- With all of the schemas selected, for **Host Name**, enter the host name of the database.
- With all of the schemas selected, for **Port**, enter the listening port of the database.

13. Click **Next**.

The JDBC Component Schema Test screen is displayed.

14. If the test succeeds, click **Next**.

The Advanced Configuration screen is displayed.

15. Select **System Components**.

16. Click **Next**.

17. Click **Add** to create a new Oracle HTTP Server instance.

18. Enter a name for the instance and select OHS as the component type.

19. Click **Next**.

20. The fields in the OHS Server page are prepopulated.

21. Click **Next**.

22. If you do not want to create a new machine, in the Machines page, click **Next**.

23. In the Assign System Components page, double-click the server to move it under the machine.

24. Review the information on the screen and if it is correct, click **Update**.

25. When the operation completes, click **Done**.

19.3 Adding Additional Managed Servers to a Domain

You can add Managed Servers to a domain to increase the capacity of your system. The Managed Servers can be added to a cluster.

When a Managed Server is added to a cluster, it inherits the applications and services that are targeted to the cluster. When a Managed Server is not added as a part of a cluster, it does not automatically inherit the applications and services from the template.

To add a Managed Server to a domain, you can use Fusion Middleware Control, the Oracle WebLogic Server Administration Console, or WLST.

See: *Oracle WebLogic Server Administration Console Online Help* and *WLST Command Reference for WebLogic Server* for complete information about adding Managed Servers.

To add a Managed Server to a domain using the Fusion Middleware Control:

1. From the WebLogic Domain menu, choose **Administration**, then, **Create/Delete Components**.

The Create Components page is displayed.

2. Click **Create**, and select **WebLogic Server**.

The Create WebLogic Server page is displayed.

3. For **Name**, enter a name for the server.

Each server within a domain must have a name that is unique for all configuration objects in the domain. Within a domain, each server, computer, cluster, JDBC connection pool, virtual host, and any other resource type must be named uniquely and must not use the same name as the domain.

4. For **Listen Port**, enter the port number from which you want to access the server instance.

If you run multiple server instances on a single computer, each server must use its own listen port.

5. Select either **Create new WebLogic Machine** or **Select Existing WebLogic Machine**. If you select **Select Existing WebLogic Machine**, select a machine from the table.

6. Specify whether this server is to be a standalone server or a member of an existing cluster:

- If this server is to be part of an existing cluster, select the cluster.
- If this server is to be a standalone server, do not select a cluster.

7. Click **Create**.

8. If the server or cluster did not have Oracle JRF applied, apply JRF, as described in [Section 19.3.1](#).

19.3.1 Applying Oracle JRF Template to a Managed Server or Cluster

Oracle JRF (Java Required Files) consists of those components not included in the Oracle WebLogic Server installation and that provide common functionality for Oracle business applications and application frameworks.

Oracle JRF consists of several independently developed libraries and applications that are deployed into a common location. The components that are considered part of Java Required Files include Oracle Application Development Framework shared libraries and ODL logging handlers.

You must apply the JRF template to a Managed Server or cluster in certain circumstances. You can only apply JRF to Managed Servers that are in a domain in which JRF was configured. That is, you must have selected Oracle JRF in the Configuration Wizard when you created or extended the domain.

Note the following points about applying JRF:

- When you add a Managed Server to an existing cluster that is already configured with JRF, you do not need to apply JRF to the Managed Server.
- When you add a Managed Server to a domain and the Managed Server requires JRF services, but the Managed Server is not part of a cluster, you must apply JRF to the Managed Server.
- When you create a new cluster and the cluster requires JRF, you must apply JRF to the cluster.
- You do not need to apply JRF to Managed Servers that are added by product templates during the template extension process (though you must select JRF in the Configuration Wizard).
- You must restart the server or cluster after you apply JRF.

Note that if you start the server or cluster using Node Manager (for example, through the Administration Console, which uses Node Manager), you must set the Node Manager property `startScriptEnabled` to `true`. For more information, see [Section 2.7.1](#).

- If you create a server using Fusion Middleware Control, the JRF template is automatically applied.

You use the custom WLST command `applyJRF` to configure the Managed Servers or cluster with JRF. To use the custom WLST commands, you must invoke the WLST script from the Oracle Common home. See [Section 2.4.2](#) for more information.

The format of the `applyJRF` command is:

```
applyJRF(target={server_name | cluster_name | *}, domainDir=domain_path,
         [shouldUpdateDomain= {true | false}])
```

You can use the `applyJRF` command online or offline:

- In online mode, the JRF changes are implicitly activated if you use the `shouldUpdateDomain` option with the value `true` (which is the default.) In online mode, this option calls the online WLST `save()` and `activate()` commands.
- In offline mode, you must restart the Administration Server and the Managed Servers or cluster. (In offline mode, if you specify the `shouldUpdateDomain` option with the value `true`, this option calls the WLST `updateDomain()` command.)

For example, to configure the Managed Server `server1` with JRF, use the following command:

```
applyJRF(target='server1', domainDir='DOMAIN_HOME')
```

To configure all Managed servers in the domain with JRF, specify an asterisk (*) as the value of the `target` option.

To configure a cluster with JRF, use the following command:

```
applyJRF(target='cluster1', domainDir='DOMAIN_HOME')
```

See Also:

- "Java Required Files Custom WLST Commands" in the *WLST Command Reference for Infrastructure Components*
- [Section H.2.2](#) to use a different version of Spring than that which is supplied with JRF

19.4 Creating Clusters

A WebLogic Server **cluster** consists of multiple WebLogic Server server instances running simultaneously and working together to provide increased scalability and reliability. A cluster appears to clients to be a single WebLogic Server instance. The server instances that constitute a cluster can run on the same computer, or be located on different computers. You can increase a cluster's capacity by adding additional server instances to the cluster on an existing computer, or you can add computers to the cluster to host the incremental server instances. Each server instance in a cluster must run the same version of WebLogic Server.

You can create a cluster of Managed Servers using WLST, the Oracle WebLogic Server Administration Console, or Fusion Middleware Control. This section describes how to create a cluster using Fusion Middleware Control.

To create a cluster of two Managed Servers, `wls_server1` and `wls_server2`:

1. From the WebLogic Domain menu, choose **Administration**, then, **Create/Delete Components**.
The Fusion Middleware Components page is displayed.
2. Choose **Create**, then **WebLogic Cluster**.
The Create WebLogic Cluster page is displayed.
3. For **Name**, enter a name for the cluster.
4. In the Cluster Messaging Mode section, select one of the following:
 - **Unicast**. Then, for **Unicast Broadcast Channel**, enter a channel. This channel is used to transmit messages within the cluster.
 - **Multicast**. Then, for **Multicast Broadcast Channel**, enter a channel. A multicast address is an IP address in the range from 224.0.0.0 to 239.255.255.255. For **Multicast Port**, enter a port number.

Note: You must ensure that the multicast address is not in use.

5. In the Servers section, select one or more servers to be added to the cluster. In this scenario, select `wls_server1` and `wls_server2`.
6. Click **Create**.

Now, you have a cluster with two members, `wls_server1` and `wls_server2`.

See Also: *Administering Clusters for Oracle WebLogic Server* for more information about clusters

19.5 Creating a Standalone Domain and a System Component

You can create a standalone domain for system components, such as Oracle HTTP Server, using the Configuration Wizard as described in "Configuring Oracle HTTP Server in a Standalone Domain" in *Installing and Configuring Oracle HTTP Server*.

Alternatively, you can use WLST to create a standalone domain, that contains a system component, for example, for Oracle HTTP Server:

1. Invoke WLST from the following directory:

```
cd ORACLE_HOME/ohs/common/bin
./wlst.sh
```

2. Read the standalone domain template. For example, for the Oracle HTTP Server standalone domain template:

```
readTemplate('ORACLE_HOME/ohs/common/templates/wls/base_standalone.jar')
addTemplate('ORACLE_HOME/ohs/common/templates/wls/ohs_standalone_template_12.1.3.jar')
```

3. Configure Node Manager:

```
cd('/')
create(domainName, 'SecurityConfiguration')
cd('SecurityConfiguration/domain_name')
set('NodeManagerUsername', 'username')
set('NodeManagerPasswordEncrypted', 'password')
setOption('NodeManagerType', 'PerDomainNodeManager')
```

4. The standalone template contains default configuration values. However, you can change those values. For example:

```
cd('/OHS/ohs1')
cmo.setAdminHost('127.0.0.1')
cmo.setAdminPort('7779')
cmo.setListenAddress('localhost')
cmo.setListenPort('7777')
cmo.setSSLListenPort('4443')
```

5. Create the domain. Note that this operation takes some time.

```
writeDomain(domain_dir)
closeTemplate()
```

19.6 Creating a System Component Instance in a WebLogic Server Domain

You can create a system component instance, such as Oracle HTTP Server, in a WebLogic Server domain using the Configuration Wizard as described in "Configuring Oracle HTTP Server in a WebLogic Server Domain" in *Installing and Configuring Oracle HTTP Server*.

Alternatively, you can create a system component instance, for example Oracle HTTP Server in the following ways:

- Using Fusion Middleware Control. For example, to create an Oracle HTTP Server instance, see "Creating an Instance by Using Fusion Middleware Control" in *Administering Oracle HTTP Server*.

- For Oracle HTTP Server using the WLST `createOHSInstance` command, as described in "Creating an Instance by Using WLST" in *Administering Oracle HTTP Server*.
- Using WLST commands, as described in this section.

This section describes how to create a system component instance using WLST commands. It uses Oracle HTTP Server as an example and assumes that you have created a WebLogic Server domain that contains Oracle JRF.

1. Invoke WLST from the following directory:

```
cd ORACLE_HOME/ohs/common/bin
./wlst.sh
```

2. Read the domain template and add the template for the system component. The following example shows the Oracle HTTP Server template:

```
readDomain('DOMAIN_HOME')
addTemplate('ORACLE_HOME/ohs/common/templates/wls/ohs_managed_template_12.1.3.jar')
```

3. If you have not already created a machine for the system component, create one:

```
cd('/')
create('ohs_machine', 'Machine')
cd('/Machines/ohs_machine')

create('ohs_machine', 'NodeManager')
cd('NodeManager/ohs_machine')
```

In this case, leave the Node Manager port as it is.

4. Create the system component instance, in this case, Oracle HTTP Server:

```
cd('/')
create('myohs', 'SystemComponent')
cd('/SystemComponent/myohs')
cmo.setComponentType('OHS')
set('Machine', 'ohs_machine')
```

5. Configure the system component instance that you just created. Note that the properties that you set will be different for each type of system component. For example, for Oracle HTTP Server:

```
cd('/OHS/myohs')
cmo.setAdminHost('127.0.0.1')
cmo.setAdminPort('7779')
cmo.setListenPort('7777')
cmo.setSSLListenPort('4443')
```

6. Update the domain:

```
updateDomain()
closeDomain()
```

19.7 Copying an Oracle Home or Component

You can copy an Oracle home or many Oracle Fusion Middleware components to a different location while preserving its configuration. Some situations in which copying Oracle Fusion Middleware is useful are:

- Creating an Oracle home that is a copy of a production, test, or development environment, enabling you to create a new Oracle home or component with all patches applied to it in a single step. This is in contrast to separately installing, configuring and applying any patches to separate components.
- Preparing a "gold" image of a patched home and deploying it to many hosts.

For information about the procedures you use to copy an Oracle home or component, see [Chapter 20](#).

Moving from a Test to a Production Environment

This chapter describes how to move Oracle Fusion Middleware from a source environment, such as a test environment, to a target environment, such as a production environment. You can develop and test applications in a source environment, and then eventually roll out the test applications and, optionally, test data to your target environment. You can also use this approach for testing and rolling out upgrades.

This chapter includes the following sections:

- Section 20.1, "Introduction to Moving Oracle Fusion Middleware Components"
- Section 20.2, "Planning for Moving Your Environment"
- Section 20.3, "Common Procedures for Moving to a Target Environment"
- Section 20.4, "Additional Steps or Information for Certain Components"
- Section 20.5, "Incrementally Moving Artifacts"
- Section 20.6, "Moving Distributed Topologies"
- Section 20.7, "Recovering from Test to Production Errors"

Note:

- The procedures in this chapter are valid for Oracle Fusion Middleware 12c (12.1.3) and the components that are part of that release.
- The procedures in this chapter for the most part assume that you are using the standard installation topology, which consists of a WebLogic Server domain that contains an Administration Server and a cluster containing two Managed Servers or a standalone domain.

For more information about the standard topology, see "Understanding the Oracle Fusion Middleware Infrastructure Standard Installation Topology" in *Installing and Configuring the Oracle Fusion Middleware Infrastructure*.

20.1 Introduction to Moving Oracle Fusion Middleware Components

You can move Oracle Fusion Middleware components from a source environment to a target environment.

Moving Oracle Fusion Middleware components minimizes the amount of work that would otherwise be required to reapply all the customization and configuration changes made in one environment to another. You can install, configure, customize, and validate Oracle Fusion Middleware in a source environment. Once the system is stable and performs as desired, you can create the target environment by moving a copy of the components and their configurations from the source environment, instead of redoing all the changes that were incorporated into the source environment.

20.2 Planning for Moving Your Environment

This section describes important information that you should know before you begin moving your environment. It includes the following topics:

- [Introduction to Moving Oracle Fusion Middleware Components](#)
- [Checking the Source Environment](#)
- [Understanding How the Movement Scripts Work with Keystores](#)
- [Preparing the Target Environment](#)
- [Limitations in Moving from Source to Target](#)
- [Overview of Procedures for Moving from a Source to a Target Environment](#)

20.2.1 Introduction to the Movement Scripts

Oracle Fusion Middleware provides a series of scripts that you can use to move your environment:

- `copyBinary`: Copies the binary files of the source Oracle home.
- `pasteBinary`: Applies the copied Oracle home to the target.
- `copyConfig`: Used for any of the following:
 - Copies the configuration of a WebLogic Server domain, including any Java components or system components in the domain.
 - Copies the configuration of a standalone domain, including any system components in the domain.
 - Copies the configuration of Node Manager.
- `extractMovePlan`: Extracts a move plan as an .xml file (called `moveplan.xml`) and other files from the archive file created by the `copyConfig` operation.
- `pasteConfig`: Used for any of the following:
 - Applies the copied configuration of a WebLogic Server domain, including any Java components or system components in the domain.
 - Applies the copied configuration of a standalone domain, including any system components in the domain.
 - Applies the copied configuration of Node Manager.

The scripts enable you to copy an Oracle home and Oracle WebLogic Server domains, as well as the configuration of certain Oracle Fusion Middleware components, such as Oracle HTTP Server and Oracle SOA Suite.

[Table 20–1](#) shows which Oracle Fusion Middleware components support the movement scripts.

Table 20–1 Support for Movement Scripts

Component	Supported?
Oracle SOA Core Extensions	Yes
Oracle Application Development Framework	Yes
Oracle B2B	Yes
Oracle B2B for Healthcare	Yes
Oracle Business Activity Monitoring	Yes
Oracle Business Process Management	Yes
Oracle Coherence	Yes
Oracle Data Integrator	Yes
Oracle Enterprise Data Quality	Yes
Oracle Enterprise Scheduler	Yes
Oracle HTTP Server	Yes
Oracle HTTP Server WebGate	Yes
Oracle Managed File Transfer	Yes
Oracle Platform Security Services	Yes
Oracle Service Bus	Yes
Oracle SOA Suite	Yes
Oracle User Messaging Service	Yes
Oracle Web Services Manager	Yes
Oracle WebLogic Server	Yes

For the move plan properties for components, see [Table A–11](#).

20.2.2 Checking the Source Environment

The procedures in this chapter assume that you have installed and configured Oracle Fusion Middleware on the source environment, including some or all of the following:

- Installed one or more databases to be used by Oracle Fusion Middleware components, such as Oracle SOA Suite.
- Created the needed schemas in the source environment using RCU. See *Creating Schemas with the Repository Creation Utility*.
- Installed and configured Oracle Fusion Middleware products. For example, you have installed Oracle WebLogic Server and Oracle Web Services Manager, created the Oracle home, and configured an Oracle WebLogic Server domain.

When you configure the domain, you can choose one of two modes:

- Development mode: In this mode, the security configuration is relatively relaxed. User name and password are required to deploy applications.
 - Production mode: In this mode, the security configuration is relatively stringent, requiring a user name and password to deploy applications and to start the Administration Server.
- Alternatively, you have installed and configured system components, such as Oracle HTTP Server, in a standalone domain.

- Configured security policies.
- For Oracle Platform Security Services, created security policies and stored credentials in the Credential Store Framework (CSF).
- Deployed one or more applications or SOA Composite applications. The applications may have internal and external references.
- Before you execute the copyConfig script in a WebLogic Server domain, make sure that the Administration Server and Managed Servers are running.
- On Windows, before you execute the copyConfig script in a WebLogic Server domain, you must shut down Node Manager.
- For Oracle Web Services Manager, before you execute the copyConfig script, the server on which the Oracle Web Services Manager Policy Manager application is deployed must be running.

Also, note the following about the source environment:

- Before you execute the copyConfig script in a WebLogic Server domain, make sure that the Administration Server and Managed Servers are running.
- On Windows, before you execute the copyConfig script in a WebLogic Server domain, you must shut down Node Manager.
- For Oracle Web Services Manager, before you execute the copyConfig script, the server on which the Oracle Web Services Manager Policy Manager application is deployed must be running.

20.2.3 Understanding How the Movement Scripts Work with Keystores

Oracle Fusion Middleware supports two types of keystores:

- JKS: Java Keystore
- KSS: Oracle Platform Security Services Keystore Service. The Keystore Service is available only if you created a domain that includes Oracle JRF.

Keystore-related properties are populated for all servers in the move plan in the following circumstances:

- If SSL is enabled (either the Administration Server port or the SSL port of the Administration Server) in the source domain, irrespective of which keystores configured.
- If only non-SSL ports are enabled in the source domain and the keystores of the Administration Server are one of the following types:
 - CustomIdentityandCustomTrust
 - CustomIdentityandJavaStandardTrust
 - CustomIdentityandCommandLineTrust
- If only non-SSL ports are enabled and DemoIdentityAndDemoTrust keystores are configured in the source domain, the keystore-related properties are not populated in the move plan.

Irrespective of how the source environment is configured, note the following about how the move plan properties must be configured before you move the configuration to the target using the pasteConfig script:

- For domains configured with Oracle JRF:
 - All servers must have the same keystores.

- The keystore type (JKS or KSS) must be the same across all servers.
- You can modify the move plan to change the keystore type from JKS to KSS or KSS to JKS.
- For domains not configured with Oracle JRF:
 - All servers must have the same keystores.
 - You can only use JKS keystores.
- You can change keystores from source to target both for domains configured with Oracle JRF and those configured without Oracle JRF. Except when the source is only non-SSL and DemoIdentityAndDemoTrust, you can change the value of the keystore to one of following, whatever the value of keystores are at source:
 - DemoIdentityAndDemoTrust
 - CustomIdentityAndCustomTrust
 - CustomIdentityAndJavaStandardTrust
 - CustomIdentityAndCommandLineTrust

20.2.4 Preparing the Target Environment

To use the procedures in this chapter, your target environment must meet the following prerequisites:

- You must use the cloningclient.jar file and movement scripts, such as pasteBinary, that are compatible with the version of the Oracle home and components that you want to copy. The procedures in this chapter presume that you are using the current version of the cloningclient.jar file and movement scripts.
- The target environment must be on the same operating system as the source environment. Also, the operating system architecture must be the same in both environments. For example, both environments must be running 32-bit operating systems or 64-bit operating systems.
- When you execute the scripts, you must specify a matching Java home. That is, if the Oracle homes are 64 bit, you must specify a 64-bit Java home. If the Oracle homes are 32 bit, you must specify a 32-bit Java home.
- The host must have JDK 1.7.0_x or higher installed.
- The target environment must have the same superuser or administrative user as the user at the source environment. After you complete the movement of the installation, you can modify the user on the target environment.
- The database in the target environment must be the same type of database as in the source environment. For example, if the database in the source environment is an Oracle Database, the database in the target environment must be an Oracle Database. The database on the target environment should be the same version as on the source environment.
- If the database is not tuned correctly, the copyConfig and pasteConfig operations can incur performance issues. To avoid these performance issues, in addition to following standard database performance tuning guidelines, ensure that you have sufficient RAM allocated for your database for the import of the MDS tables. Also run statistics against the target database by executing the following procedure:

```
BEGIN
dbms_stats.gather_schema_stats(ownname => 'prefix_MDS',
METHOD_OPT => 'FOR ALL COLUMNS SIZE AUTO',
```

```
CASCADE => TRUE, ESTIMATE_PERCENT => NULL);
END;
```

In the procedure, *prefix_MDS* is the MDS schema name for your installation.

- If you are applying the archive of an Oracle home on a host that does not yet have Oracle Fusion Middleware installed, note the following:

- Copy the `pasteBinary` script from the following location in the source host to the target host:

```
(UNIX) ORACLE_HOME/oracle_common/bin/pasteBinary.sh
(Windows) ORACLE_HOME\oracle_common\bin\pasteBinary.cmd
```

Note that on Windows, you do not copy `pasteBinary.sh`.

- Copy the following file in the source host to the target host:

```
(UNIX) ORACLE_HOME/oracle_common/jlib/cloningclient.jar
(Windows) ORACLE_HOME\oracle_common\jlib\cloningclient.jar
```

- If you run the `pasteBinary` script from a different location than `ORACLE_HOME/oracle_common/bin`, then the `pasteBinary` script and the `cloningclient.jar` file must be in the same directory.

If you are running `pasteBinary` on a host that has no prior Oracle Fusion Middleware installations, `ORACLE_HOME/oracle_common/bin` will not exist prior to running `pasteBinary`, and therefore the `pasteBinary` script and `cloningclient.jar` must be in the same directory.

- Ensure that the files have execute permission.
- When you execute the `copyConfig` command on the source environment, any system components can be started or shut down. In either case, the `copyConfig` operation will complete. This pertains to both WebLogic Server domains and standalone domains.
- On Windows, the file `MSVCR90.DLL` must exist on the target host. Otherwise, `pasteConfig` will fail.

This file (or various versions of it) are located in the directory tree underneath:

```
(Windows 32 bit) C:\Windows\System32
(Windows 64 bit) C:\Windows\winsxs
```

20.2.5 Limitations in Moving from Source to Target

Note the following limitations and restrictions:

- The source and the target environment must use the same encoding. For example, if the source environment uses the encoding `ja_JP.utf8` locale and the target environment uses the encoding `ja_JP` locale, some file names may not be handled correctly in the target.
- When you move the configuration of a component, the scripts replicate the topology of the source. For example, if the source domain contains Managed Servers `server_1` and `server_2` on Host A and Managed Servers `server_3` and `server_4` on Host B, you must specify a similar relationship between Managed Servers and hosts at the target. (You specify the hosts for each Managed Server in the move plan.)

- If a custom application uses an internal data source (for example, the application was created and deployed with an internal data source using JDeveloper), the internal data source is not migrated during the pasteConfig operation.
To work around this, create an external data source in the domain, modify the application to use that data source, and deploy the application again.
- The JDK used in the source and target must be the same type.
 - The JDK used in the source and target must be the same type. For example, if the source uses Java SE, the target must use Java SE.
 - The vendor used in the source and target must be the same. For example, if the source uses an Oracle JDK, the target must use a JDK from Oracle.
 - The major version of the JDK used in the source and target must be the same. For example, if the source uses version 1.7, the target must use 1.7.
- If there is not enough space in the temporary directory when you are moving an entity, an error is returned, noting the space needed. To work around this problem, specify a different location for the temporary directory by using the T2P_JAVA_OPTIONS environment variable as described in [Section A.1.2](#).
- If you have moved your environment and executed the pasteBinary script using a custom inventory location (using the invPtrLoc parameter), you must invoke runInstaller with the following argument:


```
-invPtrLoc custom_inventory_pointer_location
```
- When you are moving Oracle Platform Security Services and the data is moving from LDAP to LDAP, the source and target LDAP domain component hierarchy must be the same. If it is not, the Oracle Platform Security Services data movement will fail. For example, if the source hierarchy is configured as `dc=us,dc=com`, the target LDAP must have the same domain component hierarchy.
- If Oracle Service Bus is configured in the domain, during the pasteConfig operation, when the Administration Server is started for the first time, you may see the following error:

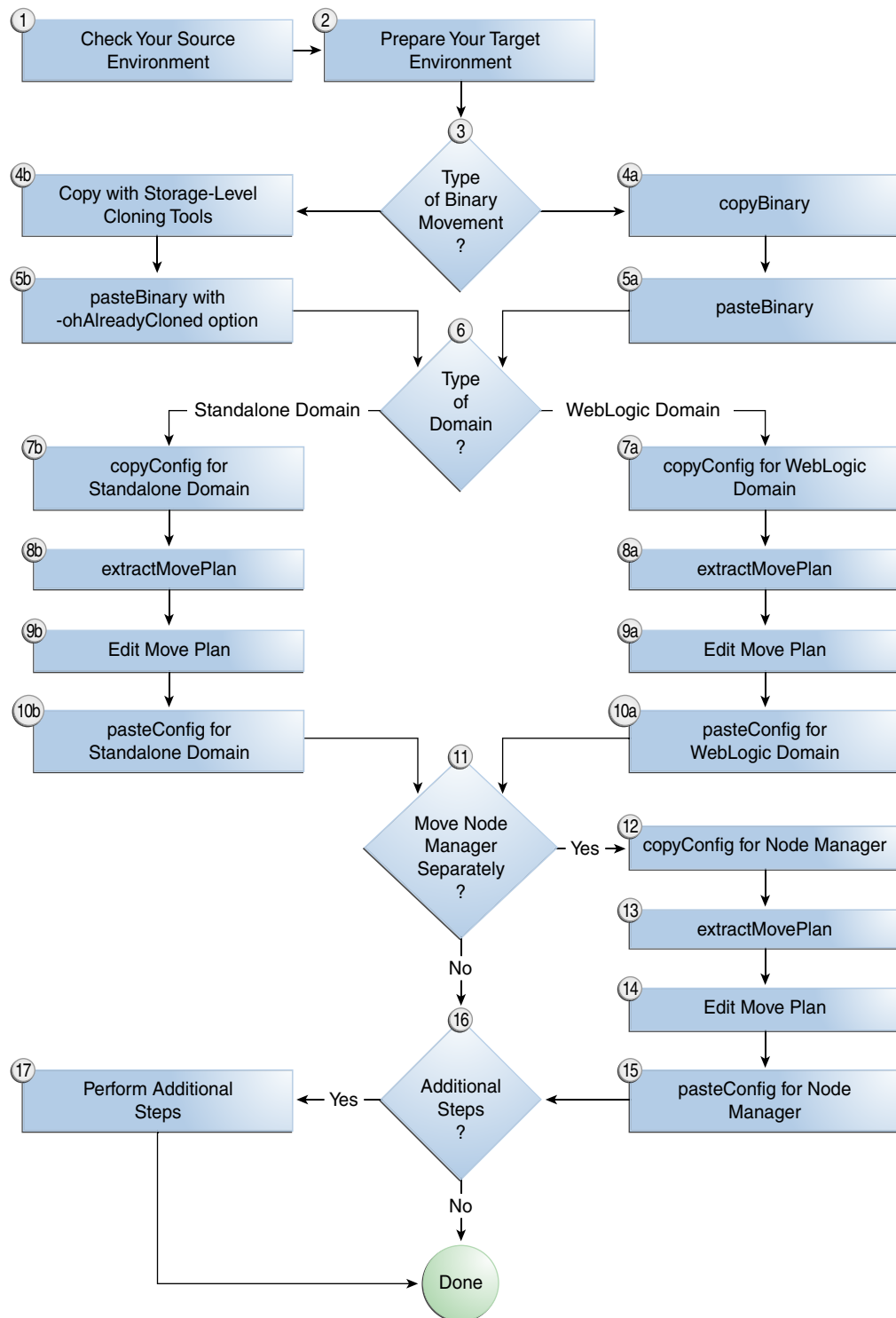

```
Failed to initialize the application "Service Bus Framework Starter
Application" due to error java.lang.RuntimeException: OSB system user
authentication failed java.lang.RuntimeException: OSB system user
authentication failed
```

You can ignore this error.

20.2.6 Overview of Procedures for Moving from a Source to a Target Environment

This section describes the general steps in moving installations from a source environment to a target environment. [Figure 20-1](#) shows a flowchart illustrating the steps.

Figure 20–1 Flowchart for Moving Your Environment



The general steps are:

1. Check your source environment. See [Section 20.2.2](#).
2. Prepare your target environment. See [Section 20.2.4](#).
3. If your environment uses a database, create a new database. See [Section 20.3.1](#).

4. Move a copy of the binary files in the Oracle home from the source environment to the target environment
 - Using the copyBinary and pasteBinary scripts, as described in [Section 20.3.2](#).
 - Using storage-level cloning tools, if supported by your environment, to create a copy of an existing disk volume and move it to a different location. Then, you use the pasteBinary script to transform the target Oracle home to a proper Oracle home, creating or updating the necessary inventory information, file permissions, and string substitutions for the correct ORACLE_HOME path. See [Section 20.3.3](#).
You can use this method if your environment is located on one disk volume.
5. Move a copy of the configuration of the domain and components. In most cases, you use the copyConfig, extractMovePlan, and pasteConfig scripts. The procedure you follow differs depending on your topology:
 - To move the configuration of a WebLogic Server domain containing only Java components, or Java components and system components, see [Section 20.3.4](#).
 - To move the configuration of a standalone domain containing system components, see [Section 20.3.5](#).
6. In certain situations, as described in [Section 20.3.6](#), you must separately move a copy of the configuration of Node Manager if it is configured in the source environment.
7. Take any additional steps that are required for some components. See [Section 20.4](#) for information specific to each component.
8. Start the servers and components. See [Section 20.3.8](#).

20.3 Common Procedures for Moving to a Target Environment

Many of the Oracle Fusion Middleware components use some of the same procedures to move from a source environment to a target environment. Note, however that not all components use all or some these procedures. In addition, some components may require additional steps. You **must** check [Table 20–2](#) to see if there are additional steps you need to take when moving a particular component.

This section describes the common procedures and contains the following topics:

- [Installing the Database on the Target Environment](#)
- [Moving the Oracle Home and the Binary Files Using the Scripts](#)
- [Moving the Oracle Home and Binary Files Using Storage-Level Cloning Tools](#)
- [Moving the Configuration of a WebLogic Server Domain](#)
- [Moving the Configuration of a Standalone Domain](#)
- [Moving the Configuration of Node Manager](#)
- [Configuring Users and Groups](#)
- [Starting Managed Servers and Components](#)

The procedures in this section assume that you are using the standard installation topology. This topology consists of a WebLogic Server domain that contains an Administration Server and a cluster of two Managed Servers on one host or a standalone domain containing system components

If you have distributed your topology across multiple machines, see [Section 20.6](#).

Note: In the scripts used in these procedures and in the move plans, you often need to provide files containing passwords. To generate a file that contains an obfuscated password, use the `obfuscatePassword` script, which is described in [Section A.1.2.10](#).

20.3.1 Installing the Database on the Target Environment

Some components, such as Oracle Application Development Framework and Oracle SOA Suite, may use a database to store metadata.

Note that the database in the target environment must be the same type of database as in the source environment. For example, if the database in the source environment is an Oracle Database, the database in the target environment must be an Oracle Database. The database on the target environment should be the same version as on the source environment.

To install a new database:

1. Install and configure the database software.
2. Create the required schemas in the target database using RCU. See *Creating Schemas with the Repository Creation Utility*.
3. Create any custom schemas used by your applications. For example, if your application uses a custom schema in the source environment, create the schema in the target environment.

20.3.2 Moving the Oracle Home and the Binary Files Using the Scripts

You can move a copy of the Oracle home to the target environment using the `copyBinary` and `pasteBinary` scripts:

- The `copyBinary` script prepares the source and creates an archive. It also records the file permissions of the Oracle home.

The archive contains the Oracle home, including the product homes, such as Oracle WebLogic Server home and the Oracle HTTP Server home.

- The `pasteBinary` script checks to see that the prerequisites are met at the destination. It extracts the files from the archive file, registers the Oracle home with the Oracle inventory.

The script then restores the file permissions and relinks any files if necessary.

Note the following:

- The `copyBinary` and `pasteBinary` scripts do not carry over all the dependencies of the source Oracle home and the product homes, such as the WebLogic Server home, such as loadable modules or application-specific libraries to the target home, because the scripts proceed by copying the Oracle home and the entire source product homes to the destination Oracle home. Any files outside the source WebLogic Server or Oracle home are not automatically copied. Hence, any applications that refer to files outside the source WebLogic Server or Oracle home may not work properly in the target home.
- When you copy an Oracle home, only the read-only portions of the Oracle home are copied. Any user configuration files, such as the `user_projects` directory, are excluded from the archive. The WebLogic Server domain is not copied. (Use the `copyConfig` and `pasteConfig` scripts to copy the domain.)
- You cannot move an Oracle Home if its path is a symbolic link.

See: [Table A-1](#) for the location of the scripts used in this section.

To move the Oracle home:

1. At the source, execute the `copyBinary` script, which copies the Oracle home and the product homes, such as the WebLogic Server home, contained within the Oracle home.

See [Section A.1.2.1](#) for the syntax of the `copyBinary` script.

For example, to copy an Oracle home that is located at `/scratch/oracle/Oracle_home1`, use the following command:

```
copyBinary.sh -javaHome /scratch/oracle/jdk1.7.7.0_17
              -archiveLoc /tmp/oh_copy.jar
              -sourceOracleHomeLoc /scratch/oracle/Oracle_home1
```

2. If you are copying the Oracle home to a different host, copy the archive file to that system, or if you are using storage-level cloning, copy the snapshot copy of the volume to the target system and mount the volume.
3. Copy the `pasteBinary` script and the `cloningclient.jar` file to the target system and ensure that they have execute permission.

The `cloningclient.jar` file is located in:

```
(UNIX) ORACLE_HOME/oracle_common/jlib/cloningclient.jar
(Windows) ORACLE_HOME\oracle_common\jlib\cloningclient.jar
```

Do **not** copy the other scripts, such as `pasteConfig`. Those scripts are generated when you extract the files, as in step 5.

4. On Linux and UNIX, if the target system does not contain any installed Oracle products, you must create an `oraInst.loc` file, specifying a group whose members are given access to write to the Oracle inventory (`oraInventory`), and where you want to put Oracle inventory. For example, the `oraInst.loc` file could contain the following:

```
inst_group=dba
inventory_loc=/scratch/oracle1/oraInventory
```

Then, if the location is not the default location, use the `-invPtrLoc` option to the `pasteBinary` script to specify the location of the `oraInst.loc` file. (For linux and AIX, the default location is `/etc/oraInst.loc`; for other UNIX platforms, it is `/var/opt/oracle/oraInst.loc`.)

5. At the target, extract the files from the archive using the `pasteBinary` script. See [Section A.1.2.2](#) for the syntax of the `pasteBinary` script.

Note: If the *parent* directory for the Oracle home does not exist, the `pasteBinary` script will create it.

The actual directory for the Oracle home (for example, `Oracle_Home_prod`) either must not exist or is an existing empty directory.

For example, to apply the archive to the directory `/scratch/oracle/ORACLE_HOME_prod`, use the following command:

```
pasteBinary.sh -javaHome /scratch/oracle/jdk1.7.0_17
              -archiveLoc /tmp/oh_copy.jar
              -targetOracleHomeLoc /scratch/oracle/ORACLE_HOME_prod
```

```
-targetOracleHomeName ORACLE_HOME_prod  
-invPtrLoc /scratch/oracle/oraInventory
```

The Oracle home is extracted to `/scratch/oracle/ORACLE_HOME_prod` and the product homes are extracted under it with the same names as that of the source product home names.

6. The `copyBinary` and `pasteBinary` scripts do not copy the `user_projects` directory. They do copy and paste other domain directories that are in the Oracle home. However, these domain directories are not functional. (Oracle recommends that you do not create domain directories under the Oracle home.)

Delete the domain directories from the target before you run the `pasteConfig` command. The `pasteConfig` script will recreate the domain directories on the target environment, as described in [Section 20.3.4](#).

7. At the target, if the Node Manager is per host and is located under the Oracle home, delete the Node Manager directory and the files in it.

In this situation, you will move the Node Manager configuration in [Section 20.3.6](#).

20.3.3 Moving the Oracle Home and Binary Files Using Storage-Level Cloning Tools

As an alternative to the `copyBinary` script, you can use storage-level cloning tools, such as Oracle Solaris ZFS or NetApp Flex Cloning, to create a copy of an existing disk volume and move it to a different location.

You can use this method if your environment is located on one disk volume.

To move the Oracle home and binary files using storage-level cloning tools:

1. Use the cloning tool to replicate the disk volume to the target environment.
Refer to the documentation for your disk volume for more specific information.
2. At the target, use the `pasteBinary` script using the `-ohAlreadyCloned` option. With this option, the `pasteBinary` script creates or updates the necessary inventory information, file permissions, and string substitutions for the correct `ORACLE_HOME` path.

See [Section A.1.2.2](#) for the syntax of the `pasteBinary` script.

For example, to apply the archive to the directory `/scratch/oracle/ORACLE_HOME_prod`, use the following command:

```
pasteBinary.sh -javaHome /scratch/oracle/jdk1.7.0_17  
               -ohAlreadyCloned true  
               -targetOracleHomeLoc /scratch/oracle/ORACLE_HOME_prod  
               -targetOracleHomeName ORACLE_HOME_prod
```

3. At the target, if the Node Manager is "per host" and is located under the Oracle home, delete the Node Manager directory and the files in it.

In this situation, you will move the Node Manager configuration in [Section 20.3.6](#).

4. Because the storage-level cloning tools copy the entire user directory, it copies not just the binary files, but also the domain directories if they have been configured in the source environment. However, these domain directories are not properly configured, so that they are not functional.

Delete the domain directories from the target before you run the `pasteConfig` command, which will recreate properly configured domain directories on the target environment, as described in [Section 20.3.4](#).

20.3.4 Moving the Configuration of a WebLogic Server Domain

You can move a copy of the WebLogic Server domain configuration using the `copyConfig`, `extractMovePlan`, and `pasteConfig` scripts. This step moves a copy of the configuration, including the domain, the Administration Server and Managed Servers and any components in the domain.

When you move the configuration of a component, the scripts replicate the topology of the source. For example, if the source domain contains Managed Servers `server_1` and `server_2` on Host A and Managed Servers `server_3` and `server_4` on Host B, you must specify a similar relationship between Managed Servers and hosts at the target. (You specify the hosts for each Managed Server in the move plan.)

The domain directory is local to each machine. The `pasteConfig` script is performed only on the Administration Server domain directory. Subsequently, if the Managed Servers are not in the same directory as the Administration Server, you must re-create the domain directory for those Managed Servers by using the Oracle WebLogic Server pack and `unpack` commands. For more information, see *Creating Templates and Domains Using the Pack and Unpack Commands*.

Because, in most cases, the user-specific data is not the same in the target environment as in the source environment, this process does not move user-specific data.

See: [Table A-1](#) for the location of the scripts used in this section.

Note: By default, during the `copyConfig` and `pasteConfig` operations, the following, which specifies the maximum heap size and the maximum permanent generation space, are set:

```
-Xmx512m -XX:MaxPermSize=256m
```

You can modify the values using the `T2P_JAVA_OPTIONS` parameter of the `copyConfig` and `pasteConfig` scripts.

To move a copy of the domain configuration:

1. At the source, make sure that the Administration Server and all Managed Servers are started.
2. On Windows, before you execute the `copyConfig` script, you must shut down Node Manager.
3. At the source, make sure that the domain configuration is not set to automatically acquire locks. If you configured the domain in development mode, automatically acquiring locks is enabled. If you configured the domain in production mode, it is disabled by default. Take the following steps:
 - a. In the Administration Console, click **Preferences**.
 - b. In the User Preferences tab, clear **Automatically Acquire Lock and Activate Changes**.
 - c. Click **Save**.
 - d. In the Change Center, click **Release Configuration**, if applicable.
4. At the source, run the following script to generate an obfuscated password file for the `domainAdminPasswordFile` parameter.

```
(UNIX) ORACLE_HOME/oracle_common/bin/obfuscatePassword.sh
      -javaHome path_to_java_home
```

```
(Windows) ORACLE_HOME\oracle_common\bin\obfuscatePassword.cmd
```

```
-javaHome path_to_java_home
```

The script prompts you to enter the password and the path, including the file name, where the password file is to be written.

5. At the source, copy the domain configuration by executing the copyConfig script.

The copyConfig script is located in:

```
(UNIX) ORACLE_HOME/oracle_common/bin/copyConfig.sh  
(Windows) ORACLE_HOME\oracle_common\bin\copyConfig.cmd
```

See [Section A.1.2.3](#) for the syntax of the copyConfig script.

For example, to copy the configuration of the domain named WLS_domain1 in the Oracle home /scratch/oracle/Oracle_home1, use the following command:

```
copyConfig.sh -javaHome /scratch/oracle/jdk1.7.0_17  
              -archiveLoc /tmp/wls.jar  
              -sourceDomainLoc /scratch/oracle/domains/WLS_domain1  
              -sourceOracleHomeLoc /scratch/oracle/Oracle_home1  
              -domainHostName example.com  
              -domainPortNum 8001  
              -domainAdminUserName domain_admin_username  
              -domainAdminPasswordFile /scratch/admin/passwd.txt  
              -logDirLoc /tmp/logs
```

For Oracle Service Bus, when you use the copyConfig script, you must pass it the `-additionalParams` option, with the key `osb.configuration.passphrase.file` and the key value specifying the absolute path to the file containing the passphrase. For example:

```
-additionalParams osb.configuration.passphrase.file=/scratch/passwd/osb_passwd
```

If you do not specify this option, the exported configuration will not be password protected.

6. If you are copying the domain configuration to a different host, copy the archive file to that system.
7. At the source, extract the move plan from the archive, using the extractMovePlan script.

See [Section A.1.2.6](#) for the syntax of the extractMovePlan script.

For example:

```
extractMovePlan.sh -javaHome /scratch/oracle/jdk1.7.7.0_17  
                  -archiveLoc /tmp/wls.jar  
                  -planDirLoc /tmp/Oracle/t2p_plans/wls
```

Note: You must extract a new move plan each time you use the copyConfig script even if no changes have been made to the source environment. The pasteConfig scripts checks that the move plan and archive match. If they do not, the script returns an error.

8. Edit the move plan, modifying the properties to reflect the values for the target environment. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment. See [Table A-11](#) to find the list of properties for the type of component you are moving.

9. Copy the edited move plan, along with any folders created by the `extractMovePlan` script, to the target. (These folders are located in the location specified by the `planDirLoc` parameter.)

During the `pasteConfig` operation, you specify the location using the `-movePlanLoc` option.

10. At the target, run the following script to generate obfuscated password files required by the move plan. Run the script for each password file.

```
(UNIX) ORACLE_HOME/oracle_common/bin/obfuscatePassword.sh -javaHome path_to_
java_home
(Windows) ORACLE_HOME\oracle_common\bin\obfuscatePassword.cmd -javaHome path_
to_java_home
```

The script prompts you to enter the password and the path, including the file name, where the password file is to be written.

11. At the target, extract the files from the archive using the `pasteConfig` script

See [Section A.1.2.7](#) for the syntax of the script.

For example, to apply the archive to the Oracle home `/scratch/oracle/Oracle_home1`, use the following command:

```
pasteConfig.sh -javaHome /scratch/oracle/jdk1.7.7.0_17
                -archiveLoc /tmp/wls.jar
                -movePlanLoc /tmp/Oracle/t2p_plans/wls/moveplan.xml
                -targetDomainLoc /scratch/oracle/config/domains/WLS_domain1
                -targetOracleHomeLoc /scratch/oracle/Oracle_home1/
                -domainAdminPasswordFile /scratch/pwd_dir/passwd.txt
```

12. If Managed Servers are not located on the same host as the Administration Server, you must re-create the domain directory for those Managed Servers by using the Oracle WebLogic Server pack and unpack commands. For more information, see *Creating Templates and Domains Using the Pack and Unpack Commands*.

When you complete this task, you may need to perform additional steps for some components, as described in [Section 20.4](#).

20.3.5 Moving the Configuration of a Standalone Domain

You can move the configuration of standalone domain containing system components. For example, you may have installed Oracle HTTP Server in a standalone domain.

See: [Table A-1](#) for the location of the scripts used in this section.

To move the configuration of a standalone domain containing system components:

1. At the source, copy the configuration by executing the `copyConfig` script.

See [Section A.1.2.4](#) for the syntax of the `copyConfig` script.

For example, to copy the configuration of the domain named `OHS_domain1` in the Oracle home `/scratch/oracle/Oracle_home1`, use the following command:

```
copyConfig.sh -javaHome /scratch/oracle/jdk1.7.0_17
                -archiveLoc /tmp/stdalone_dom.jar
                -sourceDomainLoc /scratch/oracle/domains/OHS_domain1
                -sourceOracleHomeLoc /scratch/oracle/Oracle_home1/
```

Note that you do not need to shut down Node Manager before executing this script.

2. If you are copying the configuration to a different host, copy the archive file to that system.
3. At the source, extract the move plan from the archive created by the copyConfig script, using the extractMovePlan script.

See [Section A.1.2.6](#) for the syntax of the extractMovePlan script.

For example:

```
extractMovePlan.sh -javaHome /scratch/oracle/jdk1.7.7.0_17
                  -archiveLoc /tmp/stdalone_dom.jar
                  -planDirLoc /tmp/Oracle/t2p_plans/
```

Note: You must extract a new move plan each time you use the copyConfig script even if no changes have been made to the source environment. The pasteConfig scripts checks that the move plan and archive match. If they do not, the script returns an error.

4. Edit the move plan, modifying the properties to reflect the values for the target environment. See [Table A-11](#) to find the list of properties for the type of component you are moving.
5. Copy the edited move plan, along with any folders created by the extractMovePlan script, to the target. (These folders are located in the location specified by the planDirLoc parameter.)

During the pasteConfig operation, you specify the location using the -movePlanLoc option.

6. At the target, run the following script to generate obfuscated password files required by the move plan. Run the script for each password file.

```
(UNIX) ORACLE_HOME/oracle_common/bin/obfuscatePassword.sh -javaHome path_to_
java_home
(Windows) ORACLE_HOME\oracle_common\bin\obfuscatePassword.cmd -javaHome path_
to_java_home
```

The script prompts you to enter the password and the path, including the file name, where the password file is to be written.

7. At the target, extract the files from the archive using the pasteConfig script

See [Section A.1.2.7](#) for the syntax of the script.

For example, to apply the archive to the Oracle home /scratch/oracle/Oracle_home1, use the following command:

```
pasteConfig.sh -javaHome /scratch/oracle/jdk1.7.7.0_17
               -archiveLoc /tmp/stdalone_dom.jar
               -targetDomainLoc /scratch/oracle/config/domains/dom_cl
               -targetOracleHomeLoc /scratch/oracle/Oracle_home1
               -movePlanLoc /tmp/Oracle/t2p_plans/move_plan.xml
               -logDirLoc /tmp/log
```

20.3.6 Moving the Configuration of Node Manager

If Node Manager is configured in the source environment, you must separately move Node Manager in the following circumstances:

- The Node Manager is "per host."

- In an environment on multiple hosts, the Node Manager is "per domain" and its configuration is within the domain directory, but each host has customized Node Manager properties that are applicable to only that host.

If the Node Manager is "per domain," the scripts for moving the domain also move the Node Manager.

See: [Table A-1](#) for the location of the scripts used in this section.

To move the Node Manager configuration:

1. At the source, ensure that the Node Manager is running.
2. At the source, copy the Node Manager configuration, by executing the copyConfig script.

See [Section A.1.2.5](#) for the syntax of the script. For example, use the following command:

```
copyConfig.sh -javaHome /scratch/oracle/jdk1.7.7.0_17
              -archiveLoc /tmp/nm.jar
              -sourceNMHomeLoc /scratch/oracle/Oracle_
home1/wlserver/common/nodemanager
              -logDirLoc /tmp/logs
```

3. If you are copying the Node Manager to a different host, copy the archive file to that system.
4. At the source, extract the move plan from the archive, using the extractMovePlan script.

See [Section A.1.2.6](#) for the syntax of the extractMovePlan script.

For example:

```
extractMovePlan.sh -javaHome /scratch/oracle/jdk1.7.7.0_17
                  -archiveLoc /tmp/nm.jar
                  -planDirLoc /tmp/Oracle/t2p_plans/nm
```

5. Edit the move plan, modifying the properties to reflect the values for the target environment. See [Table A-12](#) and [Table A-13](#) to find the list of properties for Node Manager.
6. Copy the edited move plan, along with any folders created by the extractMovePlan script to the target. (These folders are located in the location specified by the planDirLoc parameter.)

During the pasteConfig operation, you specify the location using the -movePlanLoc option.

7. At the target, run the following script to generate obfuscated password files required by the move plan. Run the script for each password file.

```
(UNIX) ORACLE_HOME/oracle_common/bin/obfuscatePassword.sh -javaHome path_to_
java_home
(Windows) ORACLE_HOME\oracle_common\bin\obfuscatePassword.cmd -javaHome path_
to_java_home
```

The script prompts you to enter the password and the path, including the file name, where the password file is to be written.

8. At the target, extract the files from the archive using the pasteConfig script.

See [Section A.1.2.9](#) for the syntax of the script.

For example, use the following command:

```
pasteConfig -javaHome /scratch/oracle/jdk1.7.7.0_17
            -archiveLoc /tmp/nm.jar
            -targetNMHomeLoc /scratch/oracle/Oracle_
home1/wlserver/common/nodemanager
            -targetOracleHomeLoc /scratch/oracle/Oracle_home1
            -movePlanLoc /tmp/Oracle/t2p_plans/nm/moveplan.xml
```

20.3.7 Configuring Users and Groups

You must configure security in the new target environment. The steps you take depends on the configuration of your environment and application.

The target environment LDAP identity store may not use the same users and groups as the source environment, or it may already be populated with users and groups. Take the following steps only if the LDAP store is an Oracle Internet Directory LDAP store and you need to move users, groups, and passwords from the source environment to the target environment:

1. Export the users and groups from LDAP identity store on the source environment, using the `ldapsearch` command. This produces an `ldif` file that you later import into the LDAP identity store in the target environment. The `ldapsearch` command is located in the `ORACLE_HOME/bin` directory of the Identity Management components. For example:

```
ORACLE_HOME/bin/ldapsearch -h test_oid_host -p test_oid_port
-D "cn=orcladmin" -w "test_orcladmin_passwd" -b "cn=Users,dc=us"
```

2. Import the `ldif` file that you exported from the source environment into the target environment, using the `ldapaddmt` command, as shown in the following example. (`ORACLE_HOME` is the Oracle home for Identity Management.)

```
ORACLE_HOME/bin/ldapaddmt -h production_oid_host
-p production_oid_port -D "cn=orcladmin"
-w "production_orcladmin_passwd" -r -f ldif_filename
```

20.3.8 Starting Managed Servers and Components

When the movement procedure completes, the Administration Server, Managed Servers, Node Manager, and the components are stopped. Take the following steps:

1. Start Node Manager, as described in [Section 4.2.2](#).
2. Start the Administration Server, as described in [Section 4.2.1](#).
3. Start the Managed Servers, as described in [Section 4.2.3](#)
4. Start components, as described in [Section 4.3](#).

20.4 Additional Steps or Information for Certain Components

[Table 20–2](#) shows whether any additional steps are needed to complete the movement of particular components or provides additional information.

Table 20–2 Components Requiring Additional Steps for Movement to a Different Environment

Component	Additional Procedures
Oracle Application Development Framework	None

Table 20–2 (Cont.) Components Requiring Additional Steps for Movement to a Different Environment

Component	Additional Procedures
Oracle B2B	Section 20.4.2
Oracle Business Activity Monitoring	None
Oracle Business Process Management	See Section 20.4.3
Oracle Coherence	None
Oracle Data Integrator	Section 20.4.1
Oracle Enterprise Data Quality	None
Oracle Enterprise Scheduler	None
Oracle HTTP Server	None
Oracle Managed File Transfer	None
Oracle Service Bus	See Step 5 in Section 20.3.4
Oracle SOA Core Extensions	None
Oracle SOA Suite	None
Oracle User Messaging Service	None
Oracle Web Services Manager	None
Oracle WebLogic Server	None

20.4.1 Additional Steps for Moving Oracle Data Integrator

Note the following additional steps that you must take when moving Oracle Data Integrator:

- Create the required master and work repositories schemas in the target database using RCU. See the *Creating Schemas with the Repository Creation Utility*.

Make sure that both the work and master repositories in the target environment are created with unique IDs across your entire organization, including your development and source repositories. Also make sure that the target work repository is created with the same type as the source repository (For example, if the source work repository is created as a development repository, the target work repository must also be created as a development repository).

- The ODI Work Repository Name, created as part of RCU's Custom Variables for Oracle Data Integrator, is reflected as `<configProperty id="WORKREP1">` in the `moveplan.xml` file, as shown in the following example:

```
...
<configProperty id="WORKREP1">
  <configProperty>
    <name>Url</name>
    <value>jdbc:oracle:thin:@localhost:1521:ora1120</value>
    <itemMetadata>
      <dataType>STRING</dataType>
      <scope>READ_WRITE</scope>
    </itemMetadata>
  </configProperty>
  <configProperty>
    <name>User</name>
    <value>odi_work_11g</value>
    <itemMetadata>
```

```

        <dataType>STRING</dataType>
        <scope>READ_WRITE</scope>
    </itemMetadata>
</configProperty>
<configProperty>
@    <name>Password File</name>
    <value>/tmp/all_pswd.txt</value>
    <itemMetadata>
        <dataType>STRING</dataType>
@        <password>>true</password>
        <scope>READ_WRITE</scope>
    </itemMetadata>
    </configProperty>
</configProperty>
...

```

It is important to note that if default ODI Work Repository name, WORKREP reflected as WORKREP1 in the moveplan.xml, is changed, the corresponding name change is correctly modified and followed in the production environment.

For more details about creating schemas, see *Creating Schemas with the Repository Creation Utility*. Additional information is provided in the Online Help for RCU.

- Create Projects and Models by using the ODI Client (Studio) before running the movement scripts.
- When you run the copyConfig script, note the following:
 - You must pass a configuration file to the copyConfig script when the Agent is configured. You pass this using the -additionalParams option with the argument odiCustomArg. For example:

```

./copyConfig.sh -javaHome /private/Middleware/jrocket_160_26_D1.2.0-5
               -archiveLocation /tmp/ar.jar
               -sourceOracleHomeLoc /private/Middleware
               -sourceDomainLoc /scratch/oracle/domains/base_domain
               -domainHostName host1.example.com
               -domainPortNum 7001
               -domainAdminUserName weblogic
               -domainAdminPasswordFile /tmp/wls_pswd.txt
               -additionalParams odiCustomArg=/private/t2p/odiCustomArg.xml

```

The file odiCustomArg.xml is the configuration file. A sample file is located in:

```
ORACLE_HOME/ODI_Oracle_Home/odi/plugin/t2p/odiCustomArg.xml
```

The configuration file that you pass to the script contains the connection information for all Oracle Data Integrator master repositories. The following shows a sample configuration file:

```

<?xml version="1.0" encoding="UTF-8" ?>
<config>
  <masterRepositories>
    <masterRepository>
      <driver>oracle.jdbc.OracleDriver</driver>
      <url>jdbc:oracle:thin:@localhost:1521:sid_or_service_
name/example.com</url>
      <schema>odi_master_12c</schema>
      <schema_password_file>/tmp/all_pswd.txt</schema_password_file>
      <supervisor>SUPERVISOR</supervisor>
      <supervisor_password_file>/tmp/sup_pswd.txt</supervisor_
password_file>

```



```

    </masterRepository>
    <masterRepository>
        ....content for 2nd master repository
    </masterRepository>
</masterRepositories>
</config>

```

The following explains the entries in the configuration file:

- * masterRepositories: Contains the list of ODI Master Repositories.
 - * masterRepository: The section for ODI Master Repositories.
 - * driver: The JDBC Driver to connect to the ODI Master Repository.
 - * url: The JDBC URL to connect to the ODI Master Repository.
 - * schema: The schema name for the ODI Master Repository.
 - * schema_password_file: The path for the file containing the password for the schema.
 - * supervisor: The supervisor user for the ODI Master Repository.
 - * supervisor_password_file: The path for the file containing the password for the supervisor user.
- The movement scripts update the physical architecture in the target environment according to the information you specified in the move plan. Review the following items in the physical architecture in the target environment before proceeding:
 - Physical Agents: Change the host, port, and Web application context (for Java EE Agent) to match the configuration of the target environment.
 - Data Servers: Change the data server connection information (JDBC, JNDI, data source name) to match the configuration of the target environment.
 - Physical Schemas: The schemas (including file folder location) defined for the data servers must match the configuration of the target environment.
 - After you complete the movement, restart the Java EE agents in the target environment. These agents start processing the scheduled scenarios.

20.4.2 Additional Steps for Moving Oracle B2B

Oracle B2B is moved to the target environment when you execute the movement scripts. However, you must take the following additional steps:

1. Migrate the Keystore Service certificates, as described in "Migrating Keystore Service Artifacts Within a Domain" in *Securing Applications with Oracle Platform Security Services* and update the keystore password using the B2B interface.
2. During the execution of the movement scripts, the B2B agreements are not deployed. Deploy the B2B agreements, as described in "Deploying an Agreement" in the *User's Guide for Oracle B2B*.
3. Enable the listening channel:
 - a. Log into the B2B console and select the Administration tab, then, Listening Channel.
 - b. Select the listening channel.
 - c. Select the Channel Attributes tab. Then, select **Enable Channel**.
 - d. Click **Save**.

20.4.3 Additional Steps for Moving Oracle Business Process Management

To move Oracle Business Process Management organizational units and dashboards to the new target environment:

- To create organizational units, see "Managing Organizational Units in Process Workspace" in the *Oracle Fusion Middleware Getting Started With Installation for Oracle WebLogic Server*.
- To move dashboards, use the `ant-t2p-workspace.xml` migration tool. The migration tool is available as an ant target that can be executed in the command line. It calls a configuration file that you create specifying the input parameters for the migration of data, as described in this task.

This script moves dashboards data with the `BAM_WIDGET` data type in the `BPMUserApplicationData` table to the target environment.

Note that the migration tool does not move any user-specific configuration because users in the source and target environments would not be same.

You use the following script:

```
ORACLE_HOME/soa/bin/ant-t2p-workspace.xml
```

The command has the following format:

```
ant -f ant-t2p-workspace.xml
    -Dbea.home=BEA_HOME
    -Dbpm.home=BPM_HOME
    -Dbpm.t2p.migration.config=MIGRATION_CONFIG_FILE
```

Take the following steps:

1. Ensure that the `PATH` environment variable contains the required `JAVA_HOME` and `ANT_HOME` environment variables and that they point to the locations within the Oracle SOA Suite installation.
2. Set the encryption key `oracle.bpm.services.client.key` as an environment variable. For example:

```
oracle.bpm.services.client.key=1XXXX6XXXXX98XXX
```

You can also set the encryption key by passing it as an argument to the ant command. If you do not specify it, the ant task prompts you to enter it.

3. Export dashboards from the source environment:
 - a. Create a configuration file to export dashboards:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<testToProductionMigrationConfiguration
  xmlns="http://xmlns.oracle.com/bpm/t2p/migration/config"
  xmlns:ns2="http://xmlns.oracle.com/bpm/common"
  override="true" skip="true">
  <sourceEndPoint>
    <serverEndPoint>
      <serverURL>t3://host:port</serverURL>
      <adminUserLogin>admin_username</adminUserLogin>
      <adminUserPassword>admin_password</adminUserPassword>
      <realm>jazn.com</realm>
    </serverEndPoint>
  </sourceEndPoint>
  <targetEndPoint>
    <fileEndPoint>
```

```

        <migrationFile>/tmp/bpm_dashboard.xml</migrationFile>
    </fileEndPoint>
</targetEndPoint>
<operation>EXPORT</operation>
<object>DASHBOARD</object>
<objectDetails>
    <login>username</login>
    <password>password</password>
    <identityContext>jazn.com</identityContext>
    <userApplicationData>
        <ownerId>username/ownerId>
        <option>CUSTOMLAYOUT</option>
    </userApplicationData>
</objectDetails>
</testToProductionMigrationConfiguration>

```

In the configuration file, you must specify the values for the source environment in the following elements:

- serverURL: The SOA server URL.
- adminUserLogin: The Administration user name.
- adminUserPassword: The password for the Administration user.
- migrationFile. The file that was generated by the export operation.
- objectDetails: The login and password elements.
- userApplicationData: The ownerID element.

b. Export dashboards, using the following command:

```

ant -f ant-t2p-workspace.xml
    -Dbea.home=BEA_HOME
    -Dbpm.home=BPM_HOME
    -Dbpm.t2p.migration.config=Dashboard_MIGRATION_CONFIG_FILE

```

4. Import dashboards:

a. Create a configuration file to import dashboards:

```

<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<testToProductionMigrationConfiguration
    xmlns="http://xmlns.oracle.com/bpm/t2p/migration/config"
    xmlns:ns2="http://xmlns.oracle.com/bpm/common"
    override="true" skip="true">
    <sourceEndPoint>
        <fileEndPoint>
            <migrationFile>/tmp/bpm_dashboard.xml</migrationFile>
        </fileEndPoint>
    </sourceEndPoint>
    <targetEndPoint>
        <serverEndPoint>
            <serverURL>t3://host:port</serverURL>
            <adminUserLogin>admin_username</adminUserLogin>
            <adminUserPassword>admin_password</adminUserPassword>
            <realm>jazn.com</realm>
        </serverEndPoint>
    </targetEndPoint>
    <operation>IMPORT</operation>
    <object>DASHBOARD</object>
    <objectDetails>
        <login>username</login>

```

```

    <password>password</password>
    <identityContext>jazn.com</identityContext>
    <userApplicationData>
      <ownerId>username/ownerId>
      <option>CUSTOMLAYOUT</option>
    </userApplicationData>
  </objectDetails>
</testToProductionMigrationConfiguration>

```

In the configuration file, you must update the following elements with the values for the target environment:

- serverURL: The SOA server URL.
- adminUserLogin: The Administration user name.
- adminUserPassword: The password for the Administration user.

The password will be encrypted when you first run the ant-t2p-workspace.xml tool.

- migrationFile: The file that was generated by the export operation.
- objectDetails: The login and password elements.

The password will be encrypted when you first run the ant-t2p-workspace.xml tool.

- userApplicationData: The ownerID element.

- b.** Import dashboards, using the following command:

```

ant -f ant-t2p-workspace.xml
    -Dbea.home=BEA_HOME
    -Ddbpm.home=BPM_HOME
    -Ddbpm.t2p.migration.config=Dashboard_MIGRATION_CONFIG_FILE

```

20.5 Incrementally Moving Artifacts

The movement scripts are intended for moving to a new target environment. They do not support moving artifacts to an already existing environment.

If you have already moved your environment to a new target, at some later time, you may want to move artifacts that have changed in your source environment to your target environment. For information about moving artifacts that have changed, see the documentation for the particular component, such as Oracle HTTP Server.

20.6 Moving Distributed Topologies

The following topics describe considerations when you have a distributed topology:

- [Considerations with a Multiple Host Environment](#)
- [Considerations in Moving to and from an Oracle RAC Environment](#)

20.6.1 Considerations with a Multiple Host Environment

If your domain is distributed across multiple hosts, you must take additional steps to complete the movement.

When you move the configuration of a component, the scripts replicate the topology of the source. For example, if the source domain contains Managed Servers server_1 and server_2 on Host A and Managed Servers server_3 and server_4 on Host B, you must

specify a similar relationship between Managed Servers and hosts at the target. (You specify the hosts for each Managed Server in the move plan.)

These steps assume that you have taken the steps in [Section 20.3](#) on the Administration Server host:

1. If you do not use shared disks, use the `pasteBinary` command to create an Oracle home on the remote host, for example, Host B. You use the same archive that you created in [Section 20.3.2](#) Step 1.

For example:

```
pasteBinary.sh -javaHome /scratch/oracle/jdk1.7.0_17
               -archiveLoc /tmp/oh_copy.jar
               -targetOracleHomeLoc /scratch/oracle/ORACLE_HOME_prod
               -targetOracleHomeName ORACLE_HOME_prod
```

2. Re-create the domain directory for the remote Managed Servers by using the Oracle WebLogic Server pack and unpack commands. For more information, see *Creating Templates and Domains Using the Pack and Unpack Commands*.

20.6.2 Considerations in Moving to and from an Oracle RAC Environment

If you are moving your environment to or from an Oracle Real Application Cluster (Oracle RAC) environment, note the following:

- If you are moving from a source environment that is not an Oracle RAC environment to a target environment that uses Oracle RAC, the move plan will have one entry for a generic data source (for example `mds-adf`.) You update the move plan to point to one of the Oracle RAC instances and complete the move from the source environment to the target environment.

Then, you configure your target environment for Oracle RAC, as described in the *High Availability Guide*, especially "Database Considerations."

- Multi data sources are moved to the target environment, even though they are not listed in the move plan.
- If you are moving from a source environment that uses Oracle RAC to a target environment that does not use Oracle RAC, the move plan will have multiple entries for generic data sources. For example, if you have four Oracle RAC instances, you will have four generic data sources that are named `mds-adf-rac1` through `mds-adf-rac4`. You update the move plan to point all generic data sources to the single non-RAC instance in the target environment.
- If you are moving from a source environment that uses Oracle RAC to a target environment that uses Oracle RAC, but you have more Oracle RAC instances in the target environment, the move plan will have multiple entries for generic data sources. For example, if you have three Oracle RAC instances on the source environment, you will have three generic data sources that are named `mds-adf-rac1` through `mds-adf-rac3`. You have four Oracle RAC instances in the target environment. You update the move plan to point the generic data sources to the first three generic data sources in the target environment.
- If you are moving from a source environment that uses Oracle RAC to a target environment that uses Oracle RAC, but you have fewer Oracle RAC instances in the target environment, the move plan will have multiple entries for generic data sources. For example, if you have four Oracle RAC instances on the source environment, you will have four generic data sources that are named `mds-adf-rac1` through `mds-adf-rac4`. You have three Oracle RAC instances in the target environment. You update the move plan to point the first three generic data

sources to the three generic data sources in the target environment. You point the last generic data source to the third generic data source. (The third Oracle RAC instance will contain both mds-adf-rac3 and mds-adf-rac4).

Then, you can add an additional data source, as described in [Section 10.2.2.1](#).

20.7 Recovering from Test to Production Errors

When you execute the `pasteBinary` or `pasteConfig` scripts and enter incorrect information in the move plan, the scripts return an error. In some cases, the scripts may have partially completed the paste operation. To recover, take the following actions, depending on the script that returned the error:

- On Windows if you are using the Sun JDK, the `copyBinary`, `pasteBinary`, `copyConfig`, or `pasteConfig` operations may fail with the following error:

```
java.nio.channels.OverlappingFileLockException
```

In this case, use the `T2P_JAVA_OPTIONS` to set the system property `sun.nio.ch.disableSystemWideOverlappingFileLockCheck` as shown in the following example:

```
set T2P_JAVA_OPTIONS=  
-Dsun.nio.ch.disableSystemWideOverlappingFileLockCheck=true
```

Then, retry the operation.

- If you need to re-run the `pasteConfig` script and your environment includes Oracle Platform Security Services, you must recreate the OPSS schema in the target database before you re-run the script.
- If the `pasteBinary` script returns an error while moving the Oracle home directory at the target:
 1. Delete the target Oracle home.
 2. Remove the Oracle home entry from the Oracle inventory, if it is present.
 3. For Windows, remove the shortcut for the Oracle home.
- The `copyConfig` script requires that all servers be running, but that they are idle, so that no directories are being modified. If a server is not idle, the `copyConfig` script reports that the cloning operation completed successfully and the `copyConfig` error log file will remain at 0 bytes. However, the `copyConfig` standard log file will contain an error regarding writing to the `packed_domain.jar`. That error will cause the `pasteConfig` process to fail.

To work around this issue, wait for a short period of time, then retry the `copyConfig` operation again.

- If the `pasteConfig` script returns an error while moving Java components:
 1. Stop all processes related to the domain.
 2. Delete the following directories:

```
ORACLE_HOME/user_projects/domains/domain_name  
ORACLE_HOME/user_projects/applications/domain_name
```

3. Drop the schemas and re-create them using RCU.

In addition, if the Oracle Platform Security reassociation failed:

- If you are moving from a file-based store to an LDAP store, specify a different value in the move plan.
- For an LDAP store, delete the domain node.
- For a database-based store, drop the schema and re-create it using RCU.
- If you encounter an out-of-memory error when you are using the pasteConfig script, you can work around this in one of the following ways:
 - Increase the JVM heap size: Use the option -Xmx for maximum heap size, and -Xms for initial heap size. For example:

```
CONFIG_JVM_ARGS="-Xms512m -Xmx1024m"
```

- Often, the Oracle WebLogic Server domain directory structure contains some large, unnecessary files, such as large older log files. You can delete these files, then run the copyConfig and pasteConfig scripts again.
- If you encounter the following error when you are using the copyConfig script for an Oracle SOA Suite installation, use the T2P_JAVA_OPTIONS environment variable to increase the message size:

```
weblogic.socket.MaxMessageSizeExceededException: Incoming message of size:
'10000080' bytes exceeds the configured maximum of: '10000000' bytes for
protocol: 't3'.
```

You use the T2P_JAVA_OPTIONS environment variable, as described in [Section A.1](#), to pass the -Dweblogic.MaxMessageSize=20000000 property to both the copyConfig and pasteConfig scripts.

- When you use the pasteConfig operation and Oracle B2B inbound/outbound dispatcher is configured, you may receive the following error:

```
oracle.mds.exception.MDSRuntimeException: java.sql.SQLException: Data Source
mds-soa does not exist.
Data Source mds-soa does not exist.
```

In this situation, after the failure, kill the Managed Server process and manually restart the Managed Server.

- If you receive an error when you attempt to start the Oracle SOA Suite Managed Server, you must modify system parameters using the Administration Console after you run the pasteConfig script. (Note that the pasteConfig script sets these system parameters with temporary values.)
 - a. Log into the Oracle WebLogic Server Administration Console.
 - b. In the Domain Structure window, expand the **Environment**.
 - c. Click **Servers**. The Summary of Servers page appears.
 - d. Select the server.
 - e. Select the Server Start tab.
 - f. In the **Arguments** field, enter the following parameters:

```
-Dtangosol.coherence.wkan=hostname
-Dtangosol.coherence.localhost=hostname
-Dtangosol.coherence.localport=localport_number
-Dtangosol.coherence.wka1.port=port_number_for_Coherence
```

- g. Click **Save and Activate Changes**.

- h.** Start the server.

Part IX

Appendixes

This part contains the following appendixes:

- [Appendix A, "Movement Scripts and Move Plans"](#)
- [Appendix B, "Oracle Fusion Middleware Command-Line Tools"](#)
- [Appendix C, "URLs for Components"](#)
- [Appendix D, "Port Numbers"](#)
- [Appendix E, "Using Oracle Fusion Middleware Accessibility Options"](#)
- [Appendix F, "Viewing Release Numbers"](#)
- [Appendix G, "orapki"](#)
- [Appendix H, "Troubleshooting Oracle Fusion Middleware"](#)

Movement Scripts and Move Plans

Oracle Fusion Middleware provides a series of scripts that you can use to move your environment, for example replicating a test environment to a production environment. The scripts enable you to copy an Oracle home, Oracle WebLogic Server domains and standalone domains, as well as the configuration of certain Oracle Fusion Middleware components, such as Oracle HTTP Server and Oracle SOA Suite. This appendix explains the scripts you can use to move these entities. It also describes the move plan properties that you edit when you move your environment.

This appendix contains the following sections:

- [Section A.1, "Understanding the Movement Scripts"](#)
- [Section A.2, "Modifying Move Plans"](#)

A.1 Understanding the Movement Scripts

The movement scripts copy the binary files of an Oracle home and the configuration of a domain and its components from a source environment and paste them at the target environment.

Use these scripts in conjunction with the procedures described in [Chapter 20](#).

Oracle Fusion Middleware uses the following jar file to execute the scripts necessary to move the binary and configuration files:

```
(UNIX) ORACLE_HOME/oracle_common/jlib/cloningclient.jar
(Windows) ORACLE_HOME\oracle_common\jlib\cloningclient.jar
```

[Table A-1](#) shows the scripts you use to move an Oracle home or a domain and its components.

Table A-1 *Movement Scripts*

TO:	Script	See:
Copy the binary files of the source Oracle home	(UNIX) <code>ORACLE_HOME/oracle_common/bin/copyBinary.sh</code> (Windows) <code>ORACLE_HOME\oracle_common\bin\copyBinary.cmd</code>	Section A.1.2.1
Apply the copied Oracle home to the target	(UNIX) <code>ORACLE_HOME/oracle_common/bin/pasteBinary.sh</code> (Windows) <code>ORACLE_HOME\oracle_common\bin\pasteBinary.cmd</code>	Section A.1.2.2
Copy a WebLogic Server domain and component configuration	(UNIX) <code>ORACLE_HOME/oracle_common/bin/copyConfig.sh</code> (Windows) <code>ORACLE_HOME\oracle_common\bin\copyConfig.cmd</code>	Section A.1.2.3

Table A-1 (Cont.) Movement Scripts

TO:	Script	See:
Copy a standalone domain and component configuration	(UNIX) <code>ORACLE_HOME/oracle_common/bin/copyConfig.sh</code> (Windows) <code>ORACLE_HOME\oracle_common\bin\copyConfig.cmd</code>	Section A.1.2.4
Copy the Node Manager configuration	(UNIX) <code>ORACLE_HOME/oracle_common/bin/copyConfig.sh</code> (Windows) <code>ORACLE_HOME\oracle_common\bin\copyConfig.cmd</code>	Section A.1.2.5
Extract a move plan from the domain or component	(UNIX) <code>ORACLE_HOME/oracle_common/bin/extractMovePlan.sh</code> (Windows) <code>ORACLE_HOME\oracle_common\bin\extractMovePlan.cmd</code>	Section A.1.2.6
Apply the copied configuration for the WebLogic Server domain and component configuration to the target	(UNIX) <code>ORACLE_HOME/oracle_common/bin/pasteConfig.sh</code> (Windows) <code>ORACLE_HOME\oracle_common\bin\pasteConfig.cmd</code>	Section A.1.2.7
Apply the copied standalone domain and component configuration to the target	(UNIX) <code>ORACLE_HOME/oracle_common/bin/pasteConfig.sh</code> (Windows) <code>ORACLE_HOME\oracle_common\bin\pasteConfig.cmd</code>	Section A.1.2.8
Apply the copied configuration for the Node Manager to the target	(UNIX) <code>ORACLE_HOME/oracle_common/bin/pasteConfig.sh</code> (Windows) <code>ORACLE_HOME\oracle_common\bin\pasteConfig.cmd</code>	Section A.1.2.9
Generate a file containing an obfuscated password	(UNIX) <code>ORACLE_HOME/oracle_common/bin/obfuscatePassword.sh</code> (Windows) <code>ORACLE_HOME\oracle_common\bin\obfuscatePassword.cmd</code> Note that Oracle Fusion Middleware also provides an API to generate a file containing an obfuscated password.	Section A.1.2.10

To view the help on any of these scripts, use the `-help` option. For example:

```
./pasteConfig.sh -javaHome /scratch/oracle/jdk1.7.0_17 -help
```

Note that the help shows the UNIX version of the parameter values. For other platforms, such as Windows, change the parameter values for the platform.

Note: During the `copyConfig` and `pasteConfig` operations, the following parameters, which specify the maximum heap size and the maximum permanent generation space, are set:

```
-Xmx512m  
-XX:MaxPermSize=256m
```

You can override these values using the `T2P_JAVA_OPTIONS` argument, as described in [Section A.1.1](#).

Note:

- For the temporary directory, do not provide a path that contains a space.
- A Universal Uniform Naming Convention (UNC) path is not supported on Windows. For example, the following is not supported:

```
\\host_name\oracle\java\win64\jdk6\jre\bin\java
```

This section contains the following topics:

- [Specifying Java Options](#)
- [Movement Scripts Syntax](#)

A.1.1 Specifying Java Options

To specify additional Java options, define the `T2P_JAVA_OPTIONS` environment variable and specify the options in the variable definition.

The following examples set the value for the Java temp directory:

- On Linux or UNIX:

```
setenv T2P_JAVA_OPTIONS "-Djava.io.tmpdir=/home/t2p/temp"
export T2P_JAVA_OPTIONS
```

- On Windows:

```
set T2P_JAVA_OPTIONS="-Djava.io.tmpdir=c:\home\t2p\temp"
```

Note that on Windows, the temp directory path should not contain `\x`. If it does the scripts fail.

To set the log level using `T2P_JAVA_OPTIONS`, you can use one of the following:

- Specify a configuration file to set the log level. This allows you to set the level for other log files, as well as the movement scripts log files. For example:

```
setenv T2P_JAVA_OPTIONS -Dt2p.logging.config.file=log_config_file
```

For example, the log configuration file can contain the following, which sets the level of all loggers to `FINE`, but sets the level of `org.hibernate` to `FINEST`:

```
#Root logger
.level = FINE
# Set the level of external loggers.
org.hibernate.level = FINEST
```

- Set the log level in the environment variable. For example:

```
setenv T2P_JAVA_OPTIONS -Dt2p.logging.level=level
```

The level can be one of the following: `OFF`, `SEVERE`, `WARNING`, `INFO`, `CONFIG`, `FINE`, `FINER`, `FINEST`, `ALL`.

Alternatively, the `-debug` option for the scripts sets the log level to `FINE` if the option is set to `false` (the default) or to `FINEST` if the option is set to `true`.

The precedence is as follows:

- The configuration file, set by the environment variable:
`setenv T2P_JAVA_OPTIONS -Dt2p.logging.config.file=log_config_file`
- The log level set by the environment variable:
`setenv T2P_JAVA_OPTIONS -Dt2p.logging.level=level`
- The `-debug` option on the command line.

A.1.2 Movement Scripts Syntax

The following topics describe the syntax of the movement scripts. The options are described in the tables that follow the syntax.

- [copyBinary Script](#)
- [pasteBinary Script](#)
- [copyConfig Script for Oracle WebLogic Server Domains](#)
- [copyConfig Script for Standalone Domains](#)
- [copyConfig Script for Node Manager](#)
- [extractMovePlan Script](#)
- [pasteConfig Script for Oracle WebLogic Server Domains](#)
- [pasteConfig Script for Standalone Domains](#)
- [pasteConfig Script for Node Manager](#)
- [obfuscatePassword Script and API](#)

Notes:

- Most options have shortcut names, as described in the tables later in this chapter.
- The value of options must not contain a space. For example, on Windows, you cannot pass the following as a value to the `-archiveLoc` option:

```
C:\tmp\Archive Files
```

However, the value of the `JavaHome` option can contain a space.

- On Windows, unless the command prompt uses MKS or another application to support Unix commands, and if the values contain a Windows-specific delimiter, such as an equals sign (=) or comma (,) you must wrap the entire value in double quotation marks ("). For example:

```
-additionalParams "search.encrypt.key=C:\T2P\encrypt.txt"
```

- The vendor and version of Java used in the `javaHome` option must match the vendor and version of the `JAVA_HOME` property defined in the following file (note the period (.) before the filename):

```
ORACLE_HOME/wlserver/.product.properties
```

A.1.2.1 copyBinary Script

Creates an archive file of the source Oracle home by copying the binary files of that Oracle home, including its WebLogic Server home, into the archive file.

The copyBinary script is located in:

```
(UNIX) ORACLE_HOME/oracle_common/bin/copyBinary.sh
(Windows) ORACLE_HOME\oracle_common\bin\copyBinary.cmd
```

The syntax is:

```
copyBinary -javaHome path_of_jdk
           -archiveLoc archive_location
           -sourceOracleHomeLoc ORACLE_HOME_location
           [-logDirLoc log_dir_path]
           [-silent {true | false}]
           [-ignoreDiskWarning {true | false}]
           [-debug {true | false}]
```

The following example shows how to create an archive of an Oracle home on Linux:

```
copyBinary.sh -javaHome /scratch/oracle/jdk1.7.0_17
              -archiveLoc /tmp/oh_copy.jar
              -sourceOracleHomeLoc /scratch/oracle/Oracle_home1
```

Note: When you execute the script, you must specify a matching Java home. That is, if the Oracle homes are 64 bit, you must specify a 64-bit Java home. If the Oracle homes are 32 bit, you must specify a 32-bit Java home.

Table A-2 describes the options for the copyBinary script.

Table A-2 Options for the copyBinary Script

Options	Shortcut	Description	Mandatory or Optional
-javaHome	NA	The absolute path of the Java Developer's Kit. The script detects if the operating system is 64 bit and passes the -d64 option to the scripts in the command line.	Mandatory
-archiveLoc	-al	The absolute path of the archive location. Use this option to specify the location of the archive file to be created with the copyBinary script. The archive location must not exist. Ensure that the archive location is not within the Oracle home structure.	Mandatory
-sourceOracleHomeLoc	-soh	The absolute path of the Oracle home to be archived. You can only specify one Oracle home. In previous releases, this option was sourceMWHomeLoc. That option is deprecated.	Mandatory
-invPtrLoc	-ipl	This option is deprecated. If you specify it, it will be ignored. On UNIX and Linux, the absolute path to the Oracle Inventory pointer.	Ignored
-logDirLoc	-ldl	The absolute path of a directory. The directory may or may not exist. A new log file is created in the directory. The default is the system Temp location.	Optional

Table A–2 (Cont.) Options for the copyBinary Script

Options	Shortcut	Description	Mandatory or Optional
-silent	NA	Specifies whether the operation operates silently. That is, it does not prompt for confirmation, which is the default. To specify that it does prompt for confirmation, specify this option with the value of <code>false</code> . To continue, you must type <code>yes</code> , which is not case sensitive. Typing anything other than <code>yes</code> causes the script to abort.	Optional
-ignoreDiskWarning	-idw	Specifies whether the operation ignores a warning that there is not enough free space available. The default is <code>false</code> . You may need to use this flag if the target is NFS mounted or is on a different file system, such as Data ONTAP.	Optional
-debug	NA	Sets the log level for the script to provide debugging information. The default is <code>false</code> , which sets the log level to <code>FINE</code> . If you set this to <code>true</code> , the log level is set to <code>FINEST</code> . See Section A.1.1 for other options for setting the log level.	

A.1.2.2 pasteBinary Script

Applies the archive to the target destination, by pasting the binary files of the source Oracle home to the target environment. You can apply the archive to the same host or a different host.

Before you execute this script, see [Section 20.2.4](#) for information about steps you may need to take to prepare your target environment.

The `pasteBinary` script is located in:

```
(UNIX) ORACLE_HOME/oracle_common/bin/pasteBinary.sh
(Windows) ORACLE_HOME\oracle_common\bin\pasteBinary.cmd
```

The syntax is:

```
pasteBinary -javaHome path_of_jdk
             -archiveLoc archive_location
             -targetOracleHomeLoc target_Oracle_Home_location
             [-targetOracleHomeName Oracle_home_name]
             [-ouiParam key1=value], key2=value]
             [-ohAlreadyCloned {true | false}]
             [-executeSysPrereqs {true | false}]
             [-invPtrLoc Oracle_InventoryLocation]
             [-logDirLoc log_dir_path]
             [-silent {true | false}]
             [-ignoreDiskWarning {true | false}]
             [-debug {true | false}]
```

The following example shows how to apply the archive to the directory `/scratch/oracle/Oracle_home_prod`, on Linux:

```
pasteBinary.sh -javaHome /scratch/oracle/jdk1.7.7.0_17
               -archiveLoc /tmp/oh_copy.jar
               -targetOracleHomeLoc /scratch/oracle/Oracle_home_prod
               -targetOracleHomeName Oracle_home_prod
```

[Table A–3](#) describes the options for the `pasteBinary` script.

Table A–3 Options for the pasteBinary Script

Options	Shortcut	Description	Mandatory or Optional
-javaHome	NA	The absolute path of the Java Developer's Kit. The script detects if the operating system is 64 bit and passes the -d64 option to the scripts in the command line.	Mandatory
-archiveLoc	-al	The absolute path of the archive location. Use this option to specify the location of the archive file created with the copyBinary script. The location must exist. This option is mutually exclusive with the -ohAlreadyCloned option.	Mandatory
-targetOracleHomeLoc	-toh	The absolute path of the target Oracle home. Ensure that the Oracle home directory does not exist at that location, or if it does, it is an empty directory. Otherwise, the script returns an error message. The -targetOracleHomeLoc cannot be inside another Oracle home.	Mandatory
-targetOracleHomeName	-tohn	The name for the Oracle home. This name is used to register the Oracle home with Oracle Inventory,	Optional
-ouiParam	-op	Additional variables to be passed to Oracle Universal Installer, which is run as part of this script. You must pass the variables as key=value pairs. Separate multiple variables with commas. On Windows, surround the entire value pair with double quotation marks ("").	Optional
-ohAlreadyCloned	-ohac	A flag specifying that the script reconfigure an already existing Oracle home that was created using a storage-level cloning tool. If this flag is set to true, then the target Oracle home should exist and it should contain Oracle home binaries. Valid values are true and false. The default is false. You cannot use this option when you use the -archiveLoc option.	Optional
-executeSysPrereqs	-esp	Specifies whether the pasteBinary operation checks the prerequisites of the Oracle home. The default is that it checks the prerequisites. To specify that it does not check the prerequisites, specify this option with the value false.	Optional

Table A-3 (Cont.) Options for the pasteBinary Script

Options	Shortcut	Description	Mandatory or Optional
-invPtrLoc	-ipl	<p>On UNIX and Linux, the absolute path to the Oracle Inventory pointer. Use this option if the inventory location is not in the default location, so that the operation can register the Oracle homes with the central Oracle inventory specified in the Oracle Inventory pointer file.</p> <p>If the oraInst.loc is not present at default location, you must create this file either at default location as a root user or at any other location as a root or normal user. The following shows an example of the contents of the file:</p> <pre>inventory_loc=/scratch/oraInventory inst_group=dba</pre> <p>If the directory specified as the inventory_loc does not exist, the operation will create it.</p> <p>You must have write permission to the inventory location.</p> <p>On AIX and Linux, the default location is /etc/oraInst.loc. In other UNIX platforms, the default location is /var/opt/oracle/oraInst.loc</p> <p>This parameter is only supported on UNIX. On Windows, if you specify this parameter, the script returns an error.</p>	Optional, if the inventory is in the default location. Otherwise, it is mandatory on Linux.
-logDirLoc	-ldl	The absolute path of a directory. The directory may or may not exist. A new log file is created in the directory. The default is the system Temp location.	Optional
-silent	NA	<p>Specifies whether the operation operates silently. That is, it does not prompt for confirmation, which is the default.</p> <p>To specify that it does prompt for confirmation, specify this option with the value of <code>false</code>. To continue, you must type <code>yes</code>, which is not case sensitive. Typing anything other than <code>yes</code> causes the script to abort.</p>	Optional
-ignoreDiskWarning	-idw	<p>Specifies whether the operation ignores a warning that there is not enough free space available. The default is <code>false</code>.</p> <p>You may need to use this flag if the target is NFS mounted or is on a different file system, such as Data ONTAP.</p>	Optional
-debug	NA	<p>Sets the log level for the script to provide debugging information. The default is <code>false</code>, which sets the log level to <code>FINE</code>. If you set this to <code>true</code>, the log level is set to <code>FINEST</code>.</p> <p>See Section A.1.1 for other options for setting the log level.</p>	

A.1.2.3 copyConfig Script for Oracle WebLogic Server Domains

Creates a configuration archive that contains the snapshot of the configuration of a WebLogic Server domain. The underlying components of a WebLogic Server domain retain their configuration information in different data stores, such as a file system, Oracle Metadata Services (MDS), LDAP, or a database.

You must run the copyConfig script for each WebLogic Server domain in the source environment. A configuration archive is created for each source domain.

The Administration Server and all Managed Servers in the domain must be started when you run the script.

The copyConfig script is located in:

```
(UNIX) ORACLE_HOME/oracle_common/bin/copyConfig.sh
(Windows) ORACLE_HOME\oracle_common\bin\copyConfig.cmd
```

The syntax is:

```
copyConfig -javaHome path_of_jdk
           -archiveLoc archive_location
           -sourceDomainLoc domain_location
           -sourceOracleHomeLoc Oracle_home_location
           -domainHostName domain_host_name
           -domainPortNum domain_port_number
           -domainAdminUserName domain_admin_username
           -domainAdminPasswordFile domain_admin_password_file
           [-mdsDataExport {true | false}]
           [-opssDataExport {true | false}]
           [-trustKeyStoreLoc custom_trust_keystore_path]
           [-additionalParams property1=value1[, property2=value2]
           [-logDirLoc log_dir_path]
           [-silent {true | false}]
           [-debug {true | false}]
```

The following example copies the configuration of a WebLogic Server domain:

```
copyConfig.sh -javaHome /scratch/oracle/jdk1.7.0_17
              -archiveLoc /tmp/a.jar
              -sourceDomainLoc /scratch/oracle/config/domains/WLS_domain
              -sourceOracleHomeLoc /scratch/oracle/Oracle_home1
              -domainHostName myhost.example.com
              -domainPortNum 7001
              -domainAdminUserName weblogic
              -domainAdminPasswordFile /home/oracle/password_file.txt
```

Table A-4 describes the options for the copyConfig script for Oracle WebLogic Server domains.

Table A-4 Options for the copyConfig Script for Oracle WebLogic Server Domains

Options	Shortcut	Description	Mandatory or Optional
-javaHome	NA	The absolute path of the Java Developer's Kit. The script detects if the operating system is 64 bit and passes the -d64 option to the scripts in the command line.	Mandatory
-archiveLoc	-al	The absolute path of the archive location. Use this option to specify the location of the archive file to be created by the copyConfig script.	Mandatory
-sourceDomainLoc	-sdl	The absolute path of the source domain containing the Java component. Note that on Windows, you should not include a backslash at the end of the path.	Mandatory
-sourceOracleHomeLoc	-soh	The absolute path of the source Oracle home.	Mandatory
-domainHostName	-dhn	The name of the host on which the domain is configured.	Mandatory
-domainPortNum	-dpn	The port number of the Administration Server for the domain. If the Administration port is enabled, you must specify an administration port.	Mandatory
-domainAdminUserName	-dau	The name of the administrative user for the domain.	Mandatory
-domainAdminPasswordFile	-dap	The absolute path of a secure file containing the password for the administrative user for the domain on the source environment. You must provide a password file, even if you are not changing the configuration.	Mandatory

Table A-4 (Cont.) Options for the copyConfig Script for Oracle WebLogic Server Domains

Options	Shortcut	Description	Mandatory or Optional
-mdsDataExport	-mde	Specifies whether to export the application MDS metadata to the archive so that it can be imported into the target. The default is true. Specify false if you do not want to export the application MDS metadata. If this option is set to true, the subsequent pasteConfig script that copies the component to the target imports the application MDS metadata to the target.	Optional
-opssDataExport	-ode	Specifies whether to export the Oracle Platform Security Services data. The default is true. If this option is set to true, the subsequent pasteConfig script that copies the component to the target imports the Oracle Platform Security Services data to the target. Note: If this option is set to true, you must set the following environment variable before you run the pasteConfig script: <code>CONFIG_JVM_ARGS "-Xmx2048M -Xms2048M"</code>	Optional
-trustKeyStoreLoc	-tkl	The absolute path of the trust keystore location. Use this parameter if the domainPortNum is an SSL port or administration port and the server is configured with CustomIdentityAndCustomTrust or CustomIdentityAndCommandLineTrust keystores.	Optional
-logDirLoc	-ldl	The absolute path of a directory. The directory may or may not exist. A new log file is created in the directory. The default is the system Temp location.	Optional
-additionalParams	-ap	An additional parameter and its value to be passed to the script. You must pass the variables as key=value pairs. Separate multiple variables with commas. On Windows, surround the entire value pair with double quotation marks ("").	Optional
-silent	NA	Specifies whether the operation operates silently. That is, it does not prompt for confirmation, which is the default. To specify that it does prompt for confirmation, specify this option with the value of <code>false</code> . To continue, you must type <code>yes</code> , which is not case sensitive. Typing anything other than <code>yes</code> causes the script to abort.	Optional
-debug	NA	Sets the log level for the script to provide debugging information. The default is <code>false</code> , which sets the log level to FINE. If you set this to true, the log level is set to FINEST. See Section A.1.1 for other options for setting the log level.	Optional

A.1.2.4 copyConfig Script for Standalone Domains

Creates a configuration archive that contains the snapshot of the configuration of a standalone domain. The underlying components of the domain retain their configuration information in different data stores, such as a file system or a database.

You must run the copyConfig script for each domain in the source environment. A configuration archive is created for each source domain.

The copyConfig script is located in:

(UNIX) `ORACLE_HOME/oracle_common/bin/copyConfig.sh`
 (Windows) `ORACLE_HOME\oracle_common\bin\copyConfig.cmd`

The syntax is:

```
copyConfig -javaHome path_of_jdk
           -archiveLoc archive_location
           -sourceDomainLoc domain_location
           -sourceOracleHomeLoc Oracle_home_location
           [-additionalParams property1=value1[, property2=value2]
           [-logDirLoc log_dir_path]
           [-silent {true | false}]
           [-debug {true | false}]
```

The following example copies the configuration of a standalone domain:

```
copyConfig.sh -javaHome /scratch/oracle/jdk1.7.0_17
              -archiveLoc /tmp/a.jar
              -sourceDomainLoc /scratch/oracle/config/domains/base_domain
              -sourceOracleHomeLoc /scratch/oracle/Oracle_home1/
```

[Table A-4](#) describes the options for the copyConfig script for standalone domains.

Table A-5 Options for the copyConfig Script for Standalone Domains

Options	Shortcut	Description	Mandatory or Optional
-javaHome	NA	The absolute path of the Java Developer's Kit. The script detects if the operating system is 64 bit and passes the -d64 option to the scripts in the command line.	Mandatory
-archiveLoc	-al	The absolute path of the archive location. Use this option to specify the location of the archive file to be created by the copyConfig script.	Mandatory
-sourceDomainLoc	-sdl	The absolute path of the source domain containing the component. Note that on Windows, you should not include a backslash at the end of the path.	Mandatory
-sourceOracleHomeLoc	-soh	The absolute path of the source Oracle home.	Mandatory
-logDirLoc	-ldl	The absolute path of a directory. The directory may or may not exist. A new log file is created in the directory. The default is the system Temp location.	Optional
-additionalParams	-ap	An additional parameter and its value to be passed to the script. You must pass the variables as key=value pairs. Separate multiple variables with commas. On Windows, surround the entire value pair with double quotation marks ("").	Optional
-silent	NA	Specifies whether the operation operates silently. That is, it does not prompt for confirmation, which is the default. To specify that it does prompt for confirmation, specify this option with the value of false. To continue, you must type yes, which is not case sensitive. Typing anything other than yes causes the script to abort.	Optional
-debug	NA	Sets the log level for the script to provide debugging information. The default is false, which sets the log level to FINE. If you set this to true, the log level is set to FINEST. See Section A.1.1 for other options for setting the log level.	

A.1.2.5 copyConfig Script for Node Manager

Creates a configuration archive that contains the snapshot of the configuration of Node Manager.

You must run the copyConfig script for each per host Node Manager in the source environment. A configuration archive is created for each source Node Manager.

Note: For a per domain Node Manager, you do not need to move it explicitly. It is moved when you move the domain.

The copyConfig script is located in:

```
(UNIX) ORACLE_HOME/oracle_common/bin/copyConfig.sh
(Windows) ORACLE_HOME\oracle_common\bin\copyConfig.cmd
```

The syntax is:

```
copyConfig -javaHome path_of_jdk
           -archiveLoc archive_location
           -sourceNMHomeLoc source_Node_Manager_Home_location
           [-logDirLoc log_dir_path]
           [-silent {true | false}]
           [-debug {true | false}]
```

The following example shows how to create a copy of the source Node Manager configuration located in /scratch/oracle/Oracle_home1/wlserver/common/nodemanager:

```
copyConfig.sh -javaHome /scratch/oracle/jdk1.7.7.0_17
              -archiveLoc /tmp/nm.jar
              -sourceNMHomeLoc /scratch/oracle/Oracle_
home1/wlserver/common/nodemanager
```

[Table A-6](#) describes the options for the copyConfig script for Node Manager.

Table A-6 Options for the copyConfig Script for Node Manager

Options	Shortcut	Description	Mandatory or Optional
-javaHome	NA	The absolute path of the Java Developer's Kit. The script detects if the operating system is 64 bit and passes the -d64 option to the scripts in the command line.	Mandatory
-archiveLoc	-al	The absolute path of the archive location. Use this option to specify the location of the archive file to be created by the copyConfig script.	Mandatory
-sourceNMHomeLoc	-snh	The absolute path of the source Node Manager home.	Mandatory
-logDirLoc	-ldl	The absolute path of a directory. The directory may or may not exist. A new log file is created in the directory. The default is the system Temp location.	Optional

Table A-6 (Cont.) Options for the copyConfig Script for Node Manager

Options	Shortcut	Description	Mandatory or Optional
-silent	NA	Specifies whether the operation operates silently. That is, it does not prompt for confirmation, which is the default. To specify that it does prompt for confirmation, specify this option with the value of <code>false</code> . To continue, you must type <code>yes</code> , which is not case sensitive. Typing anything other than <code>yes</code> causes the script to abort.	Optional
-debug	NA	Sets the log level for the script to provide debugging information. The default is <code>false</code> , which sets the log level to <code>FINE</code> . If you set this to <code>true</code> , the log level is set to <code>FINEST</code> . See Section A.1.1 for other options for setting the log level.	

A.1.2.6 extractMovePlan Script

Extracts configuration information from the archive into a move plan. It also extracts any needed configuration plans. Then, you edit the move plan, specifying properties for the target environment.

The `extractMovePlan` script is located in:

```
(UNIX) ORACLE_HOME/oracle_common/bin/extractMovePlan.sh
(Windows) ORACLE_HOME\oracle_common\bin\extractMovePlan.cmd
```

The syntax is:

```
extractMovePlan -javaHome path_of_jdk
                -archiveLoc archive_location
                -planDirLoc move_plan_directory
                [-optimizationHints fusionApps,sameSchemaNameSinglePassword,
                rpdDataSource]
                [-logDirLoc log_dir_path]
                [-silent {true | false}]
                [-debug {true | false}]
```

The following example extracts the plans from the archive `j2ee.jar`:

```
extractMovePlan.sh -javaHome /scratch/oracle/jdk1.7.7.0_17
                  -archiveLoc /tmp/j2ee.jar
                  -planDirLoc /scratch/oracle/t2p_plans
```

The `extractMovePlan` script extracts the move plan to the specified directory. Depending on the type of component that you are moving, the `extractMovePlan` script may also extract other configuration plans. For example, it might extract the following:

```
/scratch/oracle/t2p_plans/moveplan.xml
/scratch/oracle/t2p_plans/composites/configplan1.xml
/scratch/oracle/t2p_plans/composites/configplan2.xml
/scratch/oracle/t2p_plans/adapters/deploymentplan1.xml
/scratch/oracle/t2p_plans/adapters/deploymentplan2.xml
```

[Table A-7](#) describes the options for the `extractMovePlan` script:

Table A-7 Options for the extractMovePlan Script

Options	Shortcut	Description	Mandatory or Optional
-javaHome	NA	The absolute path of the Java Developer's Kit. The script detects if the operating system is 64 bit and passes the -d64 option to the scripts in the command line.	Mandatory
-archiveLoc	-al	The absolute path of the archive location. Use this option to specify the location of the archive file created by the copyConfig script.	Mandatory
-planDirLoc	-pdl	The absolute path to a directory to which the move plan, along with any needed configuration plans, is to be extracted. The directory must not exist or, if it exists, it is empty.	Mandatory
-optimizationHints	-opth	Specifies the configuration values to auto-populate based on the topology on the target environment. These values are omitted from the move plan. You can use this option in the case of a single archive or multiple archive files. Use of the hints is recommended if they apply to your environment. This option takes the following arguments: <ul style="list-style-type: none"> fusionapps (fa). If you use the -optimizationHints option, you must provide this hint. sameSchemaNameSinglePassword (ssnsp). The same password is used for all schemas associated with a particular database. rpddataSource (rpdds). The same password is used for all schemas associated with a particular database specified in RPD_CONFIG section of the move plan. If the sameSchemaNameSinglePassword flag is provided, then this flag is automatically set to true.	Optional
-logDirLoc	-ldl	The absolute path of a directory. The directory may or may not exist. A new log file is created in the directory. The default is the system Temp location.	Optional
-silent	NA	Specifies whether the operation operates silently. That is, it does not prompt for confirmation, which is the default. To specify that it does prompt for confirmation, specify this option with the value of <code>false</code> . To continue, you must type <code>yes</code> , which is not case sensitive. Typing anything other than <code>yes</code> causes the script to abort.	Optional
-debug	NA	Sets the log level for the script to provide debugging information. The default is <code>false</code> , which sets the log level to <code>FINE</code> . If you set this to <code>true</code> , the log level is set to <code>FINEST</code> . See Section A.1.1 for other options for setting the log level.	

For information about the properties in the move plans, and which properties you should edit, see [Section A.2](#).

A.1.2.7 pasteConfig Script for Oracle WebLogic Server Domains

Applies the copied configurations from the source environment to the target environment. Inputs for the script include the location of the configuration archive created with the copyConfig script for the domain and the location of the modified move plan. The pasteConfig script re-creates the configuration information for the Oracle WebLogic Server domain in the target environment. It also merges the move plan property values for the target environment.

The pasteConfig script is located in:

(UNIX) `ORACLE_HOME/oracle_common/bin/pasteConfig.sh`
 (Windows) `ORACLE_HOME\oracle_common\bin\pasteConfig.cmd`

The syntax is:

```
pasteConfig -javaHome path_of_jdk
            -archiveLoc archive_location
            -targetDomainLoc trgt_domain_path
            -targetOracleHomeLoc trgt_Oracle_Home_path
            -movePlanLoc move_plan_path
            -domainAdminPasswordFile domain_admin_password_file
            [-appDir WLS_application_directory]
            [-logDirLoc log_dir_path]
            [-silent {true | false}]
            [-debug {true | false}]
```

The following example shows how to apply the archive of the domain to the Oracle home Oracle_home1:

```
pasteConfig.sh -javaHome /scratch/oracle/jdk1.7.7.0_17
               -archiveLoc /tmp/java_ee_cl.jar
               -targetDomainLoc /scratch/oracle/config/domains/dom_cl
               -targetOracleHomeLoc /scratch/oracle/Oracle_home1
               -movePlanLoc /scratch/oracle/java_ee/move_plan.xml
               -domainAdminPasswordFile /scratch/pwd_dir/pass.txt
               -logDirLoc /tmp/log
```

Note: If you are moving an environment that includes Oracle JRF, as in an Oracle Fusion Middleware Infrastructure installation, in the move plan, you must specify a different database for the target than is used in the source. The database host, port, service name, and schemas cannot be the same.

Table A-8 describes the options for the pasteConfig script for Oracle WebLogic Server domains.

Table A-8 Options for the pasteConfig Script for Oracle WebLogic Server Domains

Options	Shortcut	Description	Mandatory or Optional
-javaHome	NA	The absolute path of the Java Developer's Kit. The script detects if the operating system is 64 bit and passes the -d64 option to the scripts in the command line.	Mandatory
-archiveLoc	-al	The absolute path of the archive location. Use this option to specify the location of the archive file created by the copyConfig script.	Mandatory
-targetDomainLoc	-tdl	The absolute path of the target domain. The directory must not exist or, if it exists, it must be empty. The domain directory may be located outside of the directory structure of the Oracle home.	Mandatory
-targetOracleHomeLoc	-toh	The absolute path of the target Oracle home. It will be used to configure the domain.	Mandatory
-movePlanLoc	-mpl	The absolute path of the updated version of the move plan that was extracted from the source.	Mandatory

Table A–8 (Cont.) Options for the pasteConfig Script for Oracle WebLogic Server Domains

Options	Shortcut	Description	Mandatory or Optional
-domainAdminPassword File	-dap	The absolute path of a secure file containing the password for the administrative user for the domain on target environment. You must provide a password file, even if you are not changing the configuration. Note that the password is based on the authentication provider for the domain. For example, the authenticator can be an embedded LDAP or an external LDAP.	Mandatory.
-appDir	-ad	The absolute path of the Oracle WebLogic Server application directory on the target.	Optional
-logDirLoc	-ldl	The absolute path of a directory. The directory may or may not exist. A new log file is created in the directory. The default is the system Temp location.	Optional
-silent	NA	Specifies whether the operation operates silently. That is, it does not prompt for confirmation, which is the default. To specify that it does prompt for confirmation, specify this option with the value of <code>false</code> . To continue, you must type <code>yes</code> , which is not case sensitive. Typing anything other than <code>yes</code> causes the script to abort.	Optional
-debug	NA	Sets the log level for the script to provide debugging information. The default is <code>false</code> , which sets the log level to <code>FINE</code> . If you set this to <code>true</code> , the log level is set to <code>FINEST</code> . See Section A.1.1 for other options for setting the log level.	

A.1.2.8 pasteConfig Script for Standalone Domains

Applies the copied configurations from the source environment to the target environment. Inputs for the script include the location of the configuration archive created with the copyConfig script for the domain and the location of the modified move plan. The pasteConfig script re-creates the configuration information for the standalone domain in the target environment. It also merges the move plan property values for the target environment.

The pasteConfig script is located in:

```
(UNIX) ORACLE_HOME/oracle_common/bin/pasteConfig.sh
(Windows) ORACLE_HOME\oracle_common\bin\pasteConfig.cmd
```

The syntax is:

```
pasteConfig -javaHome path_of_jdk
             -archiveLoc archive_location
             -targetDomainLoc trgt_domain_path
             -targetOracleHomeLoc trgt_Oracle_Home_path
             -movePlanLoc move_plan_path
             [-appDir WLS_application_directory]
             [-logDirLoc log_dir_path]
             [-silent {true | false}]
             [-debug {true | false}]
```

The following example shows how to apply the archive of the domain to the Oracle home Oracle_home1:

```
pasteConfig.sh -javaHome /scratch/oracle/jdk1.7.7.0_17
               -archiveLoc /tmp/java_ee_cl.jar
               -targetDomainLoc /scratch/oracle/config/domains/dom_cl
```

```
-targetOracleHomeLoc /scratch/oracle/Oracle_home1
-movePlanLoc /scratch/oracle/java_ee/move_plan.xml
-logDirLoc /tmp/log
```

Table A-8 describes the options for the pasteConfig script for standalone domains.

Table A-9 Options for the pasteConfig Script for Standalone Domains

Options	Shortcut	Description	Mandatory or Optional
-javaHome	NA	The absolute path of the Java Developer's Kit. The script detects if the operating system is 64 bit and passes the -d64 option to the scripts in the command line.	Mandatory
-archiveLoc	-al	The absolute path of the archive location. Use this option to specify the location of the archive file created by the copyConfig script.	Mandatory
-targetDomainLoc	-tdl	The absolute path of the target domain. The directory must not exist or, if it exists, it must be empty. The domain directory may be located outside of the directory structure of the Oracle home.	Mandatory
-targetOracleHomeLoc	-toh	The absolute path of the target Oracle home. It will be used to configure the domain.	Mandatory
-movePlanLoc	-mpl	The absolute path of the updated version of the move plan that was extracted from the source.	Mandatory
-appDir	-ad	The absolute path of the Oracle WebLogic Server application directory on the target.	Optional
-logDirLoc	-ldl	The location of a directory. The directory may or may not exist. A new log file is created in the directory. The default is the system Temp location.	Optional
-silent	NA	Specifies whether the operation operates silently. That is, it does not prompt for confirmation, which is the default. To specify that it does prompt for confirmation, specify this option with the value of <code>false</code> . To continue, you must type <code>yes</code> , which is not case sensitive. Typing anything other than <code>yes</code> causes the script to abort.	Optional
-debug	NA	Sets the log level for the script to provide debugging information. The default is <code>false</code> , which sets the log level to <code>FINE</code> . If you set this to <code>true</code> , the log level is set to <code>FINEST</code> . See Section A.1.1 for other options for setting the log level.	

A.1.2.9 pasteConfig Script for Node Manager

Applies the copied configurations of Node Manager from the source environment to the target environment. Inputs for the script include the location of the configuration archive created with the copyConfig script for the Node Manager and the location of the modified move plan. The pasteConfig script re-creates the configuration information for Node Manager in the target environment. It also merges the move plan property values for the target environment.

Note: All the domains that are to be managed by Node Manager should be moved before applying the copy of Node Manager to the target environment. In addition, the Administration Server must be running.

You must run the `pasteConfig` script for each per host Node Manager in the target environment.

The syntax is:

```
pasteConfig -javaHome path_of_jdk
            -archiveLoc archive_location
            -targetNMHomeLoc trgt_Node_Manager_Home_path
            -targetOracleHomeLoc trgt_Oracle_Home_path
            -movePlanLoc move_plan_path
            [-logDirLoc log_dir_path]
            [-silent {true | false}]
            [-debug {true | false}]
```

The following example shows how to apply the copy of Node Manager to the Node Manager home located in `/scratch/Oracle_home1/wlserver/common/nodemanager`:

```
pasteConfig -javaHome /scratch/oracle/jdk1.7.7.0_17
            -archiveLoc /tmp/nm.jar
            -targetNMHomeLoc /scratch/oracle/Oracle_
home1/wlserver/common/nodemanager
            -targetOracleHomeLoc /scratch/oracle/Oracle_home1
            -movePlanLoc /scratch/oracle/t2pplans/nm/moveplan.xml
```

[Table A-10](#) describes the options for the `pasteConfig` script for Node Manager.

Table A-10 Options for the `pasteConfig` Script for Node Manager

Options	Shortcut	Description	Mandatory or Optional
<code>-javaHome</code>	NA	The absolute path of the Java Developer's Kit. The script detects if the operating system is 64 bit and passes the <code>-d64</code> option to the scripts in the command line.	Mandatory
<code>-archiveLoc</code>	<code>-al</code>	The absolute path of the archive location. Use this option to specify the location of the archive file created by the <code>copyConfig</code> script.	Mandatory
<code>-targetNMHomeLoc</code>	<code>-tnh</code>	The absolute path of the target Node Manager.	Mandatory
<code>-targetOracleHomeLoc</code>	<code>-toh</code>	The absolute path of the target Oracle home that will be used to configure Node Manager.	Mandatory
<code>-movePlanLoc</code>	<code>-mpl</code>	The absolute path of the modified move plan in the target environment.	Mandatory
<code>-logDirLoc</code>	<code>-ldl</code>	The absolute path of a directory. The directory may or may not exist. A new log file is created in the directory. The default is the system Temp location.	Optional
<code>-silent</code>	NA	Specifies whether the operation operates silently. That is, it does not prompt for confirmation, which is the default. To specify that it does prompt for confirmation, specify this option with the value of <code>false</code> . To continue, you must type <code>yes</code> , which is not case sensitive. Typing anything other than <code>yes</code> causes the script to abort.	Optional
<code>-debug</code>	NA	Sets the log level for the script to provide debugging information. The default is <code>false</code> , which sets the log level to <code>FINE</code> . If you set this to <code>true</code> , the log level is set to <code>FINEST</code> . See Section A.1.1 for other options for setting the log level.	

A.1.2.10 obfuscatePassword Script and API

Generates a file that contains the obfuscated password. In the scripts and in the move plans, you often need to provide files containing passwords.

The syntax is:

```
(UNIX) ORACLE_HOME/oracle_common/bin/obfuscatePassword.sh
      -javaHome path_to_java_home
(Windows) ORACLE_HOME\oracle_common\bin\obfuscatePassword.cmd
      -javaHome path_to_java_home
```

The script prompts you to enter the password and the path, including the file name, where the password file is to be written.

Alternatively, you can use an API to generate the obfuscated password file:

1. Load the following file:

```
ORACLE_HOME/oracle_common/jlib/obfuscatepassword.jar
```

2. Invoke the following API:

```
oracle.as.t2p.framework.externalutils.ObfuscatePassword.createPasswordFile(String password, String filePath)
```

A.2 Modifying Move Plans

When you move Oracle Fusion Middleware components, you run the `extractMovePlan` script to create a move plan for the entity that you are moving. The `extractMovePlan` script extracts configuration information from the archive into a move plan. It also extracts any needed configuration plans. Before you apply the archive to the target, you must edit the move plan to reflect the values of the target environment.

You can modify properties with the scope of `READ_WRITE`. Do not modify the properties with the scope of `READ_ONLY`.

Notes:

- Do not add, comment, or remove any section of a move plan.
- You must generate a move plan using the `extractMovePlan` script each time you create an archive, even if you have made no changes to the move plan. If you use a move plan that was created with a different archive, the archive will not be accepted and the `pasteConfig` script will fail.
- If the move plan properties use IP addresses, all of the addresses must use the same IP protocol format. For example, all should use the IPv4 format or all should use the IPv6 format.
- The listen address of all servers must use the same format, irrespective of how they are configured in the source file. You can use any of the following formats, but all listen addresses must use the same format:

The actual host name. For example, *hostname.domainname*

The IPv4 address

The IPv6 address

localhost

All Local Addresses

For the Oracle Coherence configuration to work properly in production mode, you must use the actual host name or the IP address, either IPv6 or IPv4, for all listen addresses in the move plan.

This section provides the following topics:

- [Locating configGroup Elements](#)
- [Move Plan Properties](#)

A.2.1 Locating configGroup Elements

Most move plans contain multiple `configGroup` elements. When a property is associated with a particular `configGroup` element, the tables that list the properties group the properties by `configGroup` element. For example, [Table A-13](#), which shows the properties for the move plan for Java components, shows multiple `configGroup` elements, such as `SERVER_CONFIG` and `MACHINE_CONFIG`.

The following example shows a portion of the move plan for Java components, with portions of the `SERVER_CONFIG` and `MACHINE_CONFIG` `configGroup` elements:

```
<?xml version="1.0" encoding="UTF-8" standalone="yes"?>
<movePlan>
  <movableComponent>
    <componentType>J2EEDomain</componentType>
    <moveDescriptor>
      <StartupMode>PRODUCTION</StartupMode>
      <configGroup>
        <type>SERVER_CONFIG</type>
        <configProperty id="Server1">
          <configProperty>
            <name>Server Name</name>
```

```

        <value>AdminServer</value>
        <itemMetadata>
            <dataType>STRING</dataType>
            <scope>READ_ONLY</scope>
        </itemMetadata>
    </configProperty>
    .
    .
    .
</configGroup>
<configGroup>
    <type>MACHINE_CONFIG</type>
    <configProperty id="Machine1">
        <configProperty>
            <name>Machine Name</name>
            <value>LocalMachine</value>
            <itemMetadata>
                <dataType>STRING</dataType>
                <scope>READ_WRITE</scope>
            </itemMetadata>
        </configProperty>
        <configProperty>
            <name>Node Manager Listen Address</name>
            <value>example.com</value>
            <itemMetadata>
                <dataType>STRING</dataType>
                <scope>READ_WRITE</scope>
            </itemMetadata>
        </configProperty>
    .
    .
    .
</configGroup>

```

A.2.2 Move Plan Properties

The tables in this section describe the move plan properties you can customize for Oracle Fusion Middleware entities and components.

Note: Many move plan properties require that you provide the location of a file containing a password. To use obfuscated passwords, you can use the `obfuscatePassword` script, as described in [Section A.1.2.10](#).

The properties that you edit differ depending on the type of component. [Table A-11](#) provides pointers to the appropriate list of properties for each component.

Table A-11 *Move Plan Properties for Components*

Component	Where to find the list of properties:
Node Manager for standalone domains	Table A-12
All Java components and Node Manager	Table A-13
Oracle ADF connections	Table A-14
Oracle B2B	Table A-23
Oracle Business Activity Monitoring	Table A-19

Table A–11 (Cont.) Move Plan Properties for Components

Component	Where to find the list of properties:
Oracle Coherence	Table A–15
Oracle Data Integrator	Table A–26
Oracle Enterprise Scheduler	Table A–24
Oracle HTTP Server	Table A–17
Oracle Managed File Transfer	Table A–25
Oracle Service Bus	Table A–21
Oracle SOA Suite	Table A–13 , Table A–14 , Table A–18
Oracle SOA Core Extensions	Table A–20
Oracle User Messaging Service	Table A–13 , Table A–14 , Table A–22
Oracle Web Services Manager	Table A–16

[Table A–12](#) describes the move plan properties that you can change for a Node Manager that is configured for a standalone domain. (Additional Node Manager properties for standalone domains and WebLogic Server domains are listed in [Table A–13](#).) Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment.

Table A–12 Move Plan Properties for Node Manager in a Standalone Domain

Property	Description	Sample Value
Properties in the NODE_MANAGER_PROPERTIES configGroup:	Node Manager configuration	
Listen Address	The Listen address of Node Manager.	example.com
Listen Port	The number of the Listen port of Node Manager.	5557
Keystores	The keystores for the Node Manager. Valid values are: <ul style="list-style-type: none"> ▪ DemoIdentityAndDemoTrust ▪ CustomIdentityAndCustomTrust ▪ CustomIdentityAndJavaStandardTrust 	DemoIdentityAndDemoTrust
Custom Identity Keystore File	The absolute path of the custom identity keystore file location. This property is present in the move plan only if the source environment is configured with SSL.	/scratch/oracle/Oracle_home1/wlserver/server/lib/example_identity.jks
Custom Identity Keystore Passphrase File	The absolute path to the secure file containing the custom identity keystore password. If the source environment uses DemoTrust, this property is optional. If left blank, the pasteConfig script shows a warning message and proceeds. If the source environment uses Custom, this property is mandatory.	/scratch/oracle/i_passwd

Table A–12 (Cont.) Move Plan Properties for Node Manager in a Standalone Domain

Property	Description	Sample Value
Custom Identity Private Key Alias	The value of the identity key store alias. This property is present in the move plan only if the source environment is configured with SSL.	mykey
Custom Identity Private Key Passphrase File	The absolute path to the secure file containing the private key used when creating a certificate. This property is present in the move plan only if the source environment is configured with SSL.	/scratch/oracle/key_passwd
Properties in the DOMAINS configGroup:	Oracle WebLogic Server domain configuration	
Domain Name	The name of the domain.	WLS_domain
Domain Location	The absolute path of the domain location.	/scratch/oracle/config/domains/WLS_domain
AdminServer Listen Address	The Listen address of the Administration Server.	example.com
AdminServer Listen Port	The number of the Listen port of the Administration Server.	7001
AdminServer User Name	The administration user name.	weblogic
AdminServer Password File	The absolute path to the secure file containing the administration user's password.	/scratch/oracle/admin_passwd
Node Manager User Name	The Node Manager user name.	weblogic
Node Manager Password File	The absolute path to the secure file containing the Node Manager user's password.	/scratch/oracle/nm_passwd
Custom Trust Keystore File	The absolute path to the secure file containing the custom trust keystore password. This property is present in the move plan only if the config property AdminServer Listen Port represents the SSL port of the server.	/scratch/oracle/trust_key_passwd

[Table A–13](#) describes the move plan properties that you can change for Java components. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment.

Table A–13 Common Move Plan Properties for Java Components

Property	Description	Sample Value
Startup Mode	No change required	
Properties in the SERVER_CONFIG configGroup:	Common Java component properties	

Table A-13 (Cont.) Common Move Plan Properties for Java Components

Property	Description	Sample Value
Keystores	<p>The keystores for all servers. This property is present only once in the move plan and pertains to all servers.</p> <p>If the value is DemoIdentityAndDemoTrust, the other keystore properties in this configGroup will be ignored.</p> <p>In this case, the value of Keystore Type will be jks for a domain not configured with Oracle JRF, or kss for a domain configured with Oracle JRF.</p>	<p>One of the following:</p> <p>DemoIdentityAndDemoTrust</p> <p>CustomIdentityAndCustomTrust</p> <p>CustomIdentityAndJavaStandardTrust</p> <p>CustomIdentityAndCommandLineTrust</p>
Keystore Type	The keystore type for all servers. This property is present only once in the move plan and pertains to all servers.	JKS or KSS
Administration Port	The port number for the Administration Server.	7001
Listen Address	The Listen address of the WebLogic Server. Set it to the host name or set it to All Local Addresses to listen on all addresses on the host.	All Local Addresses
Listen Port	<p>The number of the Listen port.</p> <p>If you do not provide a port number or if the port number you provide is not available, the operation returns an error.</p>	8001
SSL Listen Port	The number of the SSL Listen port. This property is present in the move plan if SSL is enabled.	7002
Frontend Host	<p>The host name of the HTTP Server.</p> <p>This property is present in the move plan only if the HTTP Server is set as the frontend to the server.</p>	example.com
Frontend HTTP Port	<p>The number of the HTTP Server port.</p> <p>This property is present in the move plan only if the HTTP Server is set as the frontend to the server.</p>	10605
Frontend HTTPS Port	<p>The number of the HTTPS Server port.</p> <p>This property is present in the move plan only if the HTTPS Server is set as the front end to the server.</p>	10606
Log File Location	The location of the server log file, if it is not in the default location.	/scratch/servers/ms1/ms1.log
Unicast Listen Address	<p>The unicast listen address.</p> <p>This property is present for each server that is configured for unicast.</p>	10.240.98.232
Unicast Listen Port	<p>The unicast listen port.</p> <p>This property is present for each server that is configured for unicast.</p>	7036

Table A-13 (Cont.) Common Move Plan Properties for Java Components

Property	Description	Sample Value
Default File Store Directory	<p>Controls the configuration of the default persistent store on the server.</p> <p>The default store maintains its data in a <code>data/store/default</code> directory inside the <code>servername</code> subdirectory of a domain's root directory.</p> <p>You can, however, specify another location for the default store.</p> <p>Note: This property will be populated in the move plan only if it is configured in the source environment and the path is an absolute path.</p> <p>This property is present for each server that is configured for unicast.</p>	<p><code>DOMAIN_</code> <code>HOME/servername/data/store/default</code></p>
Keystore properties	The following properties are per server.	
Custom Identity Keystore File	<p>If the keystore type is JKS, the absolute path of custom identity keystore file location. If the keystore type is KSS, the URI pattern.</p> <p>This property is mandatory if the keystores are not <code>DemoIdentityAndDemoTrust.t</code>.</p>	<p>JKS: <code>/scratch/keystores/identity.jks</code> KSS: <code>kss://appstripe/keystore</code></p>
Custom Identity Keystore Passphrase File	<p>The absolute path to the secure file containing the custom identity keystore password.</p> <p>This property is mandatory if the keystores are not <code>DemoIdentityAndDemoTrust</code>.</p>	<code>/scratch/oracle/i_passwd.txt</code>
Custom Trust Keystore File	<p>If the keystore type is JKS, the absolute path of custom trust keystore file location. If the keystore type is KSS, the URI pattern.</p> <p>This property is mandatory if the keystores are <code>CustomIdentityAndCustomTrust</code> or <code>CustomIdentityAndCommandLineTrust</code>.</p>	<p>JKS: <code>/scratch/keystores/trust.jks</code> KSS: <code>kss://appstripe/keystore</code></p>
Custom Trust Keystore Passphrase File	<p>The absolute path to the secure file containing the custom trust keystore password.</p> <p>This property is mandatory if the keystores are <code>CustomIdentityAndCustomTrust</code>.</p>	<code>/scratch/oracle/key_passwd.txt</code>
Custom Identity Private Key Alias	<p>The string alias used to store and retrieve the server's private key.</p> <p>This property is mandatory if the keystores are not <code>DemoIdentityAndDemoTrust</code>.</p>	<code>Identity_key_alias</code>
Custom Identity Private Key Passphrase File	<p>The absolute path to the secure file containing the custom identity private key password.</p> <p>This property is mandatory if the keystores are not <code>DemoIdentityAndDemoTrust</code>.</p>	<code>/scratch/oracle/i_passwd.txt</code>
IdentityKeystoreFileToBeImported	<p>The absolute path of the identity keystore file (jks file) to be imported to the Keystore service.</p> <p>This property is mandatory if the keystore type is KSS and the keystores are not <code>DemoIdentityAndDemoTrust</code>.</p>	<code>/scratch/keystores/trust.jks</code>

Table A-13 (Cont.) Common Move Plan Properties for Java Components

Property	Description	Sample Value
TrustKeystoreFileToBeImported	The absolute path of trust keystore file to be imported to the Keystore service. This property is mandatory if the keystore type is KSS and the keystores are CustomIdentityAndCustomTrust.	alias1_trust,alias2_trust
AliasesToBeImportedFromTrustKeystoreFile	A comma-separated list of aliases of the entries to be imported from the trust keystore file (specified through the property TrustKeystoreFileToBeImported) to the Keystore service. This property is mandatory if the keystore type is KSS and the keystores are CustomIdentityAndCustomTrust.	alias1_trust,alias2_trust
PasswordFilesForAliasesToBeImportedFromTrustKeystoreFile	A comma-separated list of password files containing the aliases (specified through the property AliasesToBeImportedFromTrustKeystoreFile) to be imported from the trust keystore file to Keystore service. This property is mandatory if the keystore type is KSS and the keystores are CustomIdentityAndCustomTrust.	/scratch/pass/alias1_trust_pass.txt, /scratch/pass/alias2_trust_pass.txt
Properties in the CLUSTER_CONFIG configGroup:	Oracle WebLogic Server Cluster configuration properties	
Messaging Mode	The cluster messaging mode. Acceptable values are unicast and multicast.	multicast
Cluster Address	The cluster address.	localhost
Unicast Channel	The name of the unicast channel.	MyMulticastChannel
Multicast Address	The multicast address.	239.192.0.0
Multicast Port	The port number of the multicast address.	8899
Frontend Host	The name or IP address of the front-end host for the cluster.	example.com
Frontend HTTP Port	The HTTP port number for the front-end host for the cluster.	7008
Frontend HTTPS Port	The HTTPS port number for the front-end host for the cluster.	7009
Properties in the MACHINE_CONFIG configGroup:	Machine configuration properties	
Machine Name	The name of the machine.	example.com
Node Manager Listen Address	The Listen address of the machine running Node Manager.	example.com
Node Manager Listen Port	The port number of the Listen address of the machine running Node Manager.	5556
Property in the DEPLOYMENT_PLAN_CONFIG configGroup:	Deployment plans	

Table A-13 (Cont.) Common Move Plan Properties for Java Components

Property	Description	Sample Value
Deployment Plan	The location where an application's deployment plan is to be extracted. The location is relative to the location of the move plan.	deploy_plans/helloWorldEar_plan.xml
Properties in the AUTHENTICATORS configGroup:		
Host Name	The LDAP server host name.	example.com
Port	The LDAP server port number.	3060
Principal	The administration user for the LDAP server.	cn=orcladmin
Password File	The absolute path of a secure file containing the password for the LDAP user. You must provide a password file, even if you are not changing the configuration.	/scratch/oracle/ldap_passwd.txt
User Base DN	The user base distinguished name (DN).	cn=users,dc=us,dc=oracle,dc=com
User Object Class	The user object class.	person
Group Base DN	The group base distinguished name (DN).	cn=groups,dc=us,dc=oracle,dc=com
GUID Attribute	The global unique identifier.	orclguid
Properties in the DATASOURCE configGroup:		
Driver Class	The driver class of the data source. Refer to "Using JDBC Drivers with WebLogic Server" in <i>Administering JDBC Data Sources for Oracle WebLogic Server</i> to choose the appropriate class.	oracle.jdbc.OracleDriver
Url	The URL of the database for the data source. It contains the host name, the database port number, and SID. It has the following format: jdbc:oracle:thin:@Db_host:Db_port:Db_SID	jdbc:oracle:thin:@host.example.com:1521:orcl
User	The schema name of the data source.	OFM_MDS
Password File	The absolute path to the secure file containing the password of the database schema. You must provide a password file, even if you are not changing the configuration of the data source.	/scratch/oracle/ds_passwd.txt
ONS Node List	The list of Oracle Notification Service (ONS) hosts and ports, in the following format: ons_host1:port1,ons_host2:port2	myhost1:6100,myhost2:6101
ONS Wallet File	The absolute path to the credential store file, which contains keys and certificates. This property is configured only if SSL is enabled.	/scratch/wallet
ONS Wallet Password File	The absolute path to the file containing the password for the wallet.	/scratch/ons_pass.txt

Table A–13 (Cont.) Common Move Plan Properties for Java Components

Property	Description	Sample Value
Properties in the OPSS_SECURITY configGroup, in the configProperty with the ID of LDAP.	<p>LDAP-based policy and credential store configuration.</p> <p>If the source is a file-based store, these properties, as well as the LDAP-based and database-based Policy and Credential Store properties are present in the move plan. When you configure the move plan, you can change from a file-based to an LDAP or database-based store.</p> <p>If the source is LDAP-based, only the LDAP properties are present in the move plan. You cannot change it to a different type, but you can change the LDAP endpoints.</p> <p>If the source is database-based, only the database properties are present in the move plan. You cannot change it to a different type, but you can change the database-based endpoints.</p> <p>You can only use one type of store. To use one, uncomment the section in the move plan and ensure the other is commented.</p>	
Password File	The absolute path to the secure file containing the password of the LDAP Server Administrative user. You must provide a password file, even if you are not changing the configuration of the LDAP Server.	/scratch/oracle/ldap_passwd.txt
LDAP User	The LDAP Server administrative user name.	cn=orcladmin
Jps Root	The LDAP Server context root.	cn=jpsRoot
Domain	The name of the domain.	WLS_domain
LDAP Url	The URL of the LDAP connection. It contains the host name and port number of the LDAP store.	ldap://example.com:3060
Properties in the FILESTORE_CONFIG configGroup	The configuration for the JMS file store.	
Directory	The directory for the JMS file store. If the directory is configured in the source environment to be outside the domain directory or if it is explicitly configured in the source environment and path is absolute (not relative), this property is exposed in the move plan.	/scratch/fmw/work0304/log/jms

Table A-13 (Cont.) Common Move Plan Properties for Java Components

Property	Description	Sample Value
Properties in the OPSS_SECURITY configGroup, in the configProperty with the ID of DB:	<p>Database-based policy and credential store configuration.</p> <p>If the source is a file-based store, these properties are present in the move plan. (The LDAP-based store is not present and you cannot move from a database-based to an LDAP-based store.) When you configure the move plan, you can change from a file-based to an LDAP or database-based store.</p> <p>You can only use one type of store. To use one, uncomment the section in the move plan and ensure the other is commented.</p> <p>If the source is database-based, only the database properties are present in the move plan. You cannot change it to a different type, but you can change the database-based endpoints.</p>	
Password File	The absolute path to the secure file containing the password of the OPSS schema owner. You must provide a password file, even if you are not changing the configuration.	/scratch/oracle/ldap_passwd.txt
DataSource Name	The name of the data source. The name cannot contain a slash (/).	opssds
DataSource Jndi Name	The JNDI name of the data source.	jdbc/opss
Jps Root	The LDAP Server context root.	cn=jpsRoot
Domain	The name of the domain.	WLS_domain
Driver Class	The driver class of the data source. Refer to "Selecting a JDBC Driver" in <i>Administering JDBC Data Sources for Oracle WebLogic Server</i> to choose the appropriate class.	oracle.jdbc.OracleDriver
Url	<p>The URL of the database for the data source. It contains the host name, the database port number, and SID.</p> <p>It has the following format:</p> <p><code>jdbc:oracle:thin:@Db_host:Db_port:Db_SID</code></p>	jdbc:oracle:thin:@host.example.com:1521:orcl
User	The name of the OPSS schema owner of the data source.	DEV_OPSS
Properties in the RDBMS Security Store configGroup:	Database-based security store configuration	
URL	<p>The URL of the database for the data source. It contains the host name, the database port number, and SID.</p> <p>It has the following format:</p> <p><code>jdbc:oracle:thin:@Db_host:Db_port:Db_SID</code></p>	jdbc:oracle:thin:@host.example.com:1521:orcl
Driver Class	The driver class of the RDBMS Security Store connection. Refer to "Using JDBC Drivers with WebLogic Server" in <i>Administering JDBC Data Sources for Oracle WebLogic Server</i> to choose the appropriate class.	oracle.jdbc.OracleDriver
User	The name of the schema owner.	admin

Table A-13 (Cont.) Common Move Plan Properties for Java Components

Property	Description	Sample Value
Password File	The absolute path to the secure file containing the password of the security store schema owner. You must provide a password file, even if you are not changing the configuration.	/scratch/oracle/rbms_ passwd.txt
Property in the ADAPTER configGroup:	Resource adapter configuration	
Deployment Plan	The path to the deployment plan to be used during movement to the target. The path can be absolute, or relative to the location of the move plan. The deployment plan is extracted by the extractMovePlan script.	/scratch/adapters/adapters.x ml
Properties in the Node Manager Config ConfigGroup	Node Manager configuration for the Node Manager for the Administration server host.	
Node Manager Home	The absolute location of Node Manager. This property is populated if the Node manager type is either ManualNodeManagerSetup or CustomLocationNodeManager.	/scratch/oracle/domains/base_ domain/nodemanager
Node Manager User Name	The user name for Node Manager.	weblogic
Node Manager Password File	The absolute path to a secure file containing the password for Node Manager.	/scratch/oracle/nm_pass.txt
The following properties are populated if the Node Manager type is not ManualNodeManagerSetup, and the Listen Address and Listen Port are not populated in the MACHINE_CONFIG configGroup.		
Listen Address	The Listen address of Node Manager.	example.com
Listen Port	The number of the Listen port of Node Manager.	5557
The following properties are populated if the SecureListener property in nodemanager.properties is present and not true and the Node Manager type is not ManualNodeManagerSetup.		
Keystores	The keystores for the Node Manager. Valid values are: <ul style="list-style-type: none"> ■ DemoIdentityAndDemoTrust ■ CustomIdentityAndCustomTrust ■ CustomIdentityAndJavaStandardTrust 	DemoIdentityAndDemoTrust
Custom Identity Keystore File	The absolute path of the custom identity keystore file location. This property is present in the move plan only if the source environment is configured with SSL. During pasteConfig, this property will be ignored if the keystore type is DemoIdentityAndDemoTrust.	/scratch/oracle/identity.jks or if Custom Identity Keystore type is KSS: kss:appstripe/keystore

Table A–13 (Cont.) Common Move Plan Properties for Java Components

Property	Description	Sample Value
Custom Identity Keystore Passphrase File	The absolute path to the secure file containing the custom identity keystore password. If the source environment uses DemoTrust, this property is optional. If left blank, the pasteConfig script shows a warning message and proceeds. If the source environment uses Custom, this parameters are mandatory. During pasteConfig, this property will be ignored if the keystore type is DemoIdentityAndDemoTrust.	/scratch/oracle/i_passwd.txt
Custom Identity Private Key Alias	The value of the identity key store alias. This property is present in the move plan only if the source environment is configured with SSL. During pasteConfig, this property will be ignored if the keystore type is DemoIdentityAndDemoTrust.	identity_key_alias
Custom Identity Private Key Passphrase File	The absolute path to the secure file containing the private key used when creating a certificate. This property is present in the move plan only if the source environment is configured with SSL. During pasteConfig, this property will be ignored if the keystore type is DemoIdentityAndDemoTrust.	/scratch/oracle/key_passwd
The following properties are populated in the move plan if the Node manger type is not ManualNodeManagerSetup and the CustomIdentityKeyStoreType property in nodemanager.properties is present and is KSS.	Note that the CustomIdentityKeyStoreType value can be only KSS in a JRF domain and the Node Manager type is PerDomainNodeManager.	
IdentityKeystoreFileToBeImported	The absolute path of the identity keystore file (.jks file) to be imported to the Keystore Service. This property is mandatory if the keystore type is KSS and the keystores are not DemoIdentityAndDemoTrust.	/scratch/keystores/trust.jks

[Table A–14](#) describes the move plan properties that you can change if you are using Oracle ADF connections. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment. The table is divided by component. For some components, the description column lists the OBJECT_NAME_PROPERTY type. You can search for the type to locate the relevant section.

Table A–14 Move Plan Properties for Oracle ADF Connections

Property	Description	Sample Value
Oracle ADF URL Connection	OBJECT_NAME_PROPERTY type is URLConnProvider	
Port	The port number used for the URL connections.	7000
URL	The URL used for the connection.	example.com

Table A-14 (Cont.) Move Plan Properties for Oracle ADF Connections

Property	Description	Sample Value
Oracle ADF Business Components Service Connection		
ServiceEndpointProvider	The Business Components service endpoint provider.	ADFBC
JndiFactoryInitial	The JNDI initial factory class.	com.sun.java.jndi.InitialFactory
JndiProviderUrl	The URL of the JNDI provider.	t3://example.com:7101
JndiSecurityPrincipal	The JNDI security principal name.	weblogic
WebServiceConnectionName	The Web service connection name.	test
Oracle Enterprise Scheduler		
NotificationServiceURL	The Oracle Enterprise Scheduler notification service URL.	http://localhost:8001
RequestFileDirectory	The path of the directory where request logs for jobs from OES ConcurrentProcessor (CP) extension is to be created.	/tmp/ess/requestFileDirectory
SAMLTokenPolicyURI	The SAML Policy URI to be used by CP extension.	oracle/wss11_saml_token_with_message_protection_service_policy
EssCallbackClientSecurityPolicyURI	The security policy to be used in the WS-Security headers for Web service invocations from Oracle Enterprise Scheduler for Web service callbacks.	oracle/wss11_saml_token_with_message_protection_client_policy
Oracle Business Activity Monitoring		
WEBTIER_SERVER	The Oracle BAM Web server host.	example.com
USER_NAME	The Oracle BAM user name.	user
PASSWORD	The password for the Oracle BAM user.	bam_password
WEBTIER_SERVER_PORT	The port number for the Web server.	9001
BAM_SERVER_PORT	The JNDI port number.	8001
BAM_WEBTIER_PROTOCOL	The network protocol. The valid values are HTTP and HTTPS.	HTTP
Oracle Essbase		
OBJECT_NAME_PROPERTY type is EssbaseConnProvider		
Host	The host name for the Oracle Essbase server.	example.com
Cluster	The name of the cluster of which the Oracle Essbase server is a member.	esbCluster
Port	The Listen port number of the Oracle Essbase server.	1423
Username	The user name.	user3
Oracle Web Services		
OBJECT_NAME_PROPERTY type is WebServiceConnection		

Table A–14 (Cont.) Move Plan Properties for Oracle ADF Connections

Property	Description	Sample Value
WsdlUrl	The URL for the WSDL.	http://example.com:port/MyWebService1?WSDL
Oracle Web Services	OBJECT_NAME_PROPERTY type is Port	
AddressUrl	The service endpoint URL.	http://example.com:port/MyWebService1
ProxyHost	The name of the host on which the proxy server is running.	example.com
ProxyPort	The port number to which the proxy server is listening.	80

Table A–15 describes the move plan properties that you can change for Oracle Coherence. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment.

Table A–15 Move Plan Properties for Oracle Coherence

Property	Description	Example
Properties in the COHERENCE_SERVER_CONFIG configGroup	The configuration of Oracle Coherence servers.	
Unicast Listen Address	The unicast listen address. This property is not present in the move plan if the value is localhost or a loopback address or the value is empty.	10.240.98.232
Unicast Listen Port	The unicast listen port.	7036
Properties in the COHERENCE_CLUSTER_CONFIG configGroup	The configuration of Oracle Coherence clusters.	
Custom Cluster Configuration File	An external custom configuration file used to configure this cluster.	/scratch/external_custom_config.xml
Unicast Listen Address	The unicast listen address. If the clustering mode is unicast, the properties Unicast Listen Address and Unicast Listen Port are present in the move plan. However, This property is not present in the move plan if the value of Unicast Listen Address is localhost or a loopback address or the value is empty.	10.240.98.232
Unicast Listen Port	The unicast listen port. This property is present in the move plan if the clustering mode is unicast.	7036
Multicast Listen Address	The multicast listen address. If the clustering mode is not unicast, this property is present in the move plan.	224.12.1.0
Multicast Listen Port	The multicast listen address. This property is present in the move plan if the clustering mode is not unicast.	12100
Listen Address	The listen address for the Well Known Address Name configuration property.	
Listen Port	The listen port for the Well Known Address Name configuration property	

Table A–15 (Cont.) Move Plan Properties for Oracle Coherence

Property	Description	Example
Properties in the SERVER_TEMPLATES_CONFIG configGroup	If server templates are configured, then these properties will be exposed if the coherence cluster configuration is overridden in the server templates.	
Unicast Listen Address	The unicast listen address. This property is not present in the move plan if the value is localhost or a loopback address or the value is empty.	10.240.98.232
Unicast Listen Port	The unicast listen port.	7036

Table A–16 describes the move plan properties that you can change for Oracle Web Services Manager. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment. Do not edit the value of the configProperty id.

Table A–16 Move Plan Properties for Oracle Web Services Manager

Property	Description	Sample Value
Properties in the bootstrap.configmanager componentType	The bootstrap properties used by the Oracle Web Services Manager agent to connect to the Oracle Web Services Manager Policy Manager.	
pm.url	The URL of the policy manager. If you are using the same policy manager in the target environment as in the source environment, you do not need to modify this property.	t3://example.com:7003
keystore.path	The keystore path. This can be an absolute path or a path relative to the DOMAIN_HOME/config/fmwconfig directory.	/scratch/oracle/domains/domain- name/config/fmwconfig/default- keystore.jks
truststore.path	The truststore path. This can be an absolute path or a path relative to the DOMAIN_HOME/config/fmwconfig directory.	/scratch/oracle/domains/domain- name/config/fmwconfig/default- keystore.jks
Properties in the wsm.respository componentType	The Oracle Web Services Manager repository configuration in the move plan if the Policy Manager is installed in the domain. However, if you set the -mdsDataExport parameter of the copyConfig script to false, this component type will not be present in the move plan. This component will not be present if wsm-pm is not installed in the domain.	
Properties in the configurations configGroup	The domain configuration. This configGroup is present in the move plan if applications or domains are registered in the source environment or domain configuration documents are created on the source environment. There is one configGroup per domain.	

Table A-16 (Cont.) Move Plan Properties for Oracle Web Services Manager

Property	Description	Sample Value
domain	The domain name of the context for which a configuration document is created in the repository. This property is present in the move plan when you have made changes to the default configuration for a particular context. If you do not modify this property, the configurations properties will have same context as on source environment.	domain1
wls.domain.url	The URL of the domain.	
wsdl	The WSDL created in client sub-resource document. It is used to identify the service wsdl which client invokes. This is required in Third Party Agent scenarios only.	http://host:port/sts?wsdl
KerberosLoginModule:principal	The name of the principal to be used.	HOST/localhost@example.com
KerberosLoginModule:keytab	The path to the keytab to get the secret key for the principal. This can be an absolute path or a path relative to the <i>DOMAIN_HOME</i> /config/fmwconfig directory.	./mylocation/krb5.keytab
ConfigManager:pm.url	The URL that specifies the location of the policy accessor.	t3://host.example.com:7003
ConfigManager:keystore.path	The path to the keystore. This can be an absolute path or a path relative to the <i>DOMAIN_HOME</i> /config/fmwconfig directory.	./mylocation/mykeystore.jks
ConfigManager:truststore.path	The truststore path relative to the domain configuration directory. This can be an absolute path or a path relative to the <i>DOMAIN_HOME</i> /config/fmwconfig directory.	/mylocation/mykeystore.jks
KeystoreConfig:location	The location of the keystore used for message protection. This can be an absolute path or a path relative to the <i>DOMAIN_HOME</i> /config/fmwconfig directory.	mycustomlocation/key.tab
Properties in the policysets configGroup	The configuration of policy sets. This configGroup is present in the move plan if policy sets have been created in the source environment.	
attach To	The scope of the policy sets. If the attachTo expression scope is DOMAIN or DOMAIN <i>term</i> , this property is present in the move plan. However, an exception is if it is DOMAIN(" * "). In this case, the property will not be present in the move plan.	domain1
Properties in the policies configGroup	The configuration of policies. This configGroup is present in the move plan if policies with assertions have been modified in the source environment. There can be multiple configGroups, one for each policy. The ID attribute is the name of the policy for which configGroup is created.	
wsdl-uri	The actual endpoint URI of the WSDL.	http://host:port/sts?wsdl
port-uri	The actual endpoint URI of the STS port.	http://host:port/sts-service

Table A–16 (Cont.) Move Plan Properties for Oracle Web Services Manager

Property	Description	Sample Value
sts.auth.service.principal.name	The name of the principal that should be used by the service.	HOST/localhost@EXAMPLE.COM
sts.auth.keytab.location	The location of the client's keytab file. This property is present when Security Token Service (STS) is configured with Kerberos tokens.	mycustomlocation/key.tab
sts.auth.caller.principal.name	Client's principal name.	testuser
service.principal.name	The name of the principal that should be used by the service.	HOST/localhost@EXAMPLE.COM
caller.principal.name	Client's principal name.	testuser
keytab.location	The location of the client's keytab file.	mycustomlocation/key.tab

[Table A–17](#) describes the move plan properties that you can change for Oracle HTTP Server. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment.

For Oracle HTTP Server, there are many configGroup elements in the move plan. Each configGroup element is associated with one Oracle HTTP Server configuration file. As a result, there may be more than one instance of a particular property, such as Listen.

Table A–17 Move Plan Properties for Oracle HTTP Server

Property	Description	Sample Value
Properties in the httpd.conf configGroup	The overall configuration. These properties correspond to properties in the httpd.conf file	
Listen	The Listen address. It can include the host name and port or just the port.	orcl3.example.com:8888 or 8888
ServerName	The name of the server for Oracle HTTP Server or its URL. If the host does not have a registered DNS name, use the IP address.	orcl1.example.com http://host.example.com:2222
Allow	Controls which hosts can access an area of the server. Valid values are <i>from all</i> , <i>from full_or_partial_domain_name</i> , <i>from full_or_partial_IP_address</i> , <i>from network/netmask pair</i> , <i>from network/nnn CIDR specification</i> .	from all
User	The Oracle HTTP Server administration user.	admin_user
Group	The group for the user.	admin_group1
ServerAdmin	The administrator's email address.	Webmaster@example.com
DocumentRoot	The directory that stores the main content for the Web site.	/scratch/oracle/base_domain/config/fmwconfig/components/OHS/instances/ohs_1/htdocs
SSLWallet	The location of the SSL wallet, if the wallet is not in the default location.	/scratch/oracle/base_domain/config/fmwconfig/components/OHS/ohs_1/keystores/mywallets

Table A-17 (Cont.) Move Plan Properties for Oracle HTTP Server

Property	Description	Sample Value
Properties in the ssl.conf configGroup	The SSL configuration. These properties correspond to properties in the ssl.conf file.	
Listen	The Listen address for SSL. It can include the host name and port or just the port.	orcl3.example.com:4443 or 4443
VirtualHost	The name of the virtual host. The port number listed should also be listed in the Listen property.	*.4443
Properties in the admin.conf configGroup	The administration configuration. These properties correspond to properties in the admin.conf file.	
Listen	The Listen address. It can include the host name and port or just the port.	orcl3.example.com:8888 or 8888
VirtualHost	The name of the virtual host. The port number listed should also be listed in the Listen property.	orcl3.example.com:8888
Allow	Controls which hosts can access an area of the server. Valid values are <i>from all</i> , <i>from full_or_partial_domain_name</i> , <i>from full_or_partial_IP_address</i> , <i>from network/netmask pair</i> , <i>from network/nnn CIDR specification</i> .	from all
Properties in the mod_wl_ohs configGroup	The mod_wl_ohs configuration. These properties correspond to properties in the mod_wl_ohs.conf file.	
WebLogicCluster	A comma-separated list of the host name and port of Managed Servers in the cluster	<i>host.example.com:8002,host.example.com:8003</i>
MatchExpression	A parameter that allows you to modify the values of existing parameters or add a new parameter for a particular configuration.	<i>/integration/worklistapp WebLogicHost=host.example.com WebLogicPort=23446</i>
Properties in the webgate.conf configGroup	The webgate configuration. These properties correspond to properties in the webgate.conf file.	
WebGateInstalldir	The location of the WebGate installation directory, as specified in the webgate.conf file.	<i>/scratch/oracle/oh_home/Oracle_OAMWebGate1/webgate/ohs</i>
Alias	The location of the alias, if it is not in the default location. Note that you change the value within the double quotation marks.	<i>/icons/" /scratch/orcl/icons/"</i>
ScriptAlias	The location of the script alias, if it is not in the default location. Note that you change the value within the double quotation marks.	<i>/cgi-bin/" /scratch/oraclegi-bin/"</i>
primaryOAMServerHost	The primary Oracle Access Manager server host. Note that the configuration for the secondary Oracle Access Manager server host is updated automatically the first time that WebGate communicates with the primary server.	<i>primary_oam_server_ host.example.com</i>

Table A–17 (Cont.) Move Plan Properties for Oracle HTTP Server

Property	Description	Sample Value
primaryOAMServerPort	The port number for the Oracle Access Manager primary host.	5575
Properties in the dads.conf configGroup	The configuration parameters for the PL/SQL database access descriptor. These properties correspond to properties in the dads.conf file.	
PlsqlDatabasePassword	Specific to the PLSQL module, the name of a secure file containing the password. You must provide a password file, even if you are not changing the configuration.	/scratch/orcl/plsql_passwd.txt
PlsqlDatabaseConnectionString	Specific to the PLSQL module, the service name of the database.	orcl.example.com:1521:orcl1
PlsqlNLSLanguage	Specific to the PLSQL module, the NLS_LANG variable for the database access descriptor (DAD).	America_America.UTF8

Table A–18 describes the move plan properties that you can change for Oracle SOA Suite. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment.

Table A–18 Move Plan Properties for Oracle SOA Suite

Property	Description	Sample Value
Property in the Composite configGroup:	SOA Composites configuration	
Config Plan Location	The location of the configuration plan to be used during movement to the target to redeploy the composite application. The path can be absolute, or relative to the location of the move plan. The plan is extracted during the extractMovePlan script.	/scratch/app/config_plan.xml

Table A–19 describes the move plan properties that you can change for Oracle Business Activity Monitoring. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment.

Table A–19 Move Plan Properties for Oracle Business Activity Monitoring

Property	Description	Sample Value
ApplicationURL	The URL for Oracle BAM web applications and Oracle BAM Server. Note that you do not need to update this value, unless the Oracle BAM web applications and Oracle BAM Server are deployed on separate hosts.	http://DEFAULT:0000
DURABLE_SUBSCRIBER_NAME	The durable subscriber name to be used for the EMS sample value.	myDURABLE_SUBSCRIBER_NAME
INITIAL_CONTEXT_FACTORY	The initial context factory to be used for the EMS sample value.	weblogic.jndi.WLInitialContextFactory
JNDI_URL	The JNDI URL for EMS.	t3://example.com:7001
JNDI_USERNAME	The JNDI user name.	myJMSUserName

Table A–19 (Cont.) Move Plan Properties for Oracle Business Activity Monitoring

Property	Description	Sample Value
JNDI_PASSWORD_FILE	The absolute path of a secure file containing the password. You must provide a password file, even if you are not changing the configuration.	/scratch/pass/jndi_pass.txt
JMS_USERNAME	The JMS user name.	user1
JMS_PASSWORD_FILE	The absolute path of a secure file containing the password. You must provide a password file, even if you are not changing the configuration.	/scratch/pass/jms_pass.txt

[Table A–20](#) describes the move plan properties that you can change for SOA Core Extensions. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment.

Table A–20 Move Plan Properties for SOA Core Extensions

Property	Description	Sample Value
APP_DIR	The application directory	\${fp.mds.path}
AI_HOME_NAME	The SOA Core Extensions home name.	soainfra
ODI_CONFIG_PROPERTIES_LOCATION	The location of the Oracle Data Integrator configuration properties file. This value is optional.	

[Table A–21](#) describes the move plan properties that you can change for Oracle Service Bus. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment.

Table A–21 Move Plan Properties for Oracle Service Bus

Property	Description	Sample Value
osb.configuration.passphrase.file	The absolute path to the passphrase file. The file must be accessible on the target environment. This property is required if you passed the osb.configuration.passphrase.file to the copyConfig script using the -additionalParams option. The passphrase must be the same as the one for the source environment.	/scratch/passwd/osb_passwd.txt

[Table A–22](#) describes the move plan properties that you can change for Oracle User Messaging Service. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment.

Note that you also edit the properties in [Table A–13](#). If you upgraded Oracle User Messaging Service from 11g, you must change the User property for the data source from *prefix_ORASDPM* to *prefix_UMS*. See the task "Upgrade the Schema" in *Upgrading Oracle SOA Suite and Business Process Management*.

Table A-22 Move Plan Properties for Oracle User Messaging Service

Property	Description	Sample Value
Properties for the componentType UMS:		
DefaultSenderAddress	The default address of the sender. If the UMS Message has no Sender Address of the specific DeliveryType that the driver supports, then the driver may use the DefaultSenderAddress as the Sender Address.	SMS:1234
SenderAddresses	The list of sender addresses that the driver is configured to handle. A driver with specified SenderAddresses will be selected only for an outgoing message that has a matching Sender Address. A driver that has not specified any SenderAddresses is considered to be able to handle any outgoing message regardless of the Sender Address of the message. The list should consist of UMS addresses separated by comma. The matching is case insensitive.	EMAIL:alice@example.com,EMAIL:bob@example.com.
Properties in the EmailDriver componentType:		
IncomingMailServer	The host name of the incoming mail server.	usmdemo.example.com
IncomingMailServerPort	Port number of IMAP4 (that is, 143 or 993) or POP3 (that is, 110 or 995) server.	110
IncomingUserIDs	The list of user names of the mail accounts from which the driver instance is polling. Each name must be separated by a comma, for example, user1,user2.	username.pop3@umsdemo.example.com
IncomingMailIDs	The email addresses corresponding to the user names. Each email address is separated by a comma and must reside in the same position in the list as its corresponding user name appears on the usernames list.	username.pop3@umsdemo.example.com
IncomingUserPasswords	The absolute path of a secure file containing the password. You must provide a password file, even if you are not changing the configuration. The file contains a list of passwords corresponding to the user names. Each password is separated by a comma and must reside in the same position in the list as their corresponding user name appears on the usernames list.	/scratch/oracle/ums_in_passwd.txt
OutgoingMailServer	The name of the SMTP server.	usmdemo.example.com
OutgoingMailServerPort	The port number of the SMTP server.	25
OutgoingDefaultFromAddr	The default FROM address (if one is not provided in the outgoing message).	username.pop3@umsdemo.example.com
OutgoingUsername	The user name used for SMTP authentication.	username.pop3@umsdemo.example.com

Table A–22 (Cont.) Move Plan Properties for Oracle User Messaging Service

Property	Description	Sample Value
OutgoingPassword	The absolute path of a secure file containing the password used for SMTP authentication. This is required only if SMTP authentication is supported by the SMTP server. You must provide a password file, even if you are not changing the configuration. The file includes the type of password (choose from Indirect Password/Create New User, Indirect Password/Use Existing User, and Use Cleartext Password) and Password.)	/scratch/oracle/ums_out_passwd.txt
Properties in the ExtensionEndpoint configGroup:	These properties apply to extension drivers.	
EndpointURL	Remote endpoint listener URL	http://hostname:7001/integrationtest-war/extension
mappedDomain	The extension endpoint used to deliver messages where the domain part of the recipient URI matches this value.	test
Properties in the SMPPDriver componentType:	These properties apply to SMPP drivers.	
SmsAccountId	The Account Identifier on the SMS-C.	myusername
SmsServerHost	The name (or IP address) of the SMS-C server.	example_host
TransmitterSystemId	The account ID that is used to send messages.	myusername
ReceiverSystemId	The account ID that is used to receive messages.	myusername
TransmitterSystemType	The type of transmitter system.	Logica
ReceiverSystemType	The type of receiver system.	Logica
ServerTransmitterPort	The TCP port number of the transmitter server.	9001
ServerReceiverPort	The TCP port number of the receiver server.	9001
TransmitterSystemPassword	The absolute path of a secure file containing the password of the transmitter system You must provide a password file, even if you are not changing the configuration. The file contains the type of password (choose from Indirect Password/Create New User, Indirect Password/Use Existing User, and Use Cleartext Password) and Password.)	/scratch/oracle/ums_trans_passwd.txt
ReceiverSystemPassword	The absolute path of a secure file containing the password of the receiver system You must provide a password file, even if you are not changing the configuration. The file contains the type of password (choose from Indirect Password/Create New User, Indirect Password/Use Existing User, and Use Cleartext Password) and Password.)	/scratch/oracle/ums_rec_passwd.txt
Properties in the XMPPDriver componentType:	These properties apply to XMPP drivers.	
IMServerHost	The Jabber/XMPP server host name.	example.domain.com
IMServerPort	The corresponding Jabber/XMPP server port. The default is 5222.	5222

Table A–22 (Cont.) Move Plan Properties for Oracle User Messaging Service

Property	Description	Sample Value
IMServerUsername	The Jabber/XMPP user name with which you log in. You may also enter a complete Jabber ID if its domain name is different from the Jabber/XMPP server host name.	myUserName@xmpp-domain
IMServerPassword	The absolute path of a secure file containing the corresponding password for the IMServerUsername. You must provide a password file, even if you are not changing the configuration. The file contains the type of password (choose from Indirect Password/Create New User, Indirect Password/Use Existing User, Use Cleartext Password) and Password.)	/scratch/oracle/ums_im_passwd.txt
Properties in the TwitterDriver componentType	The properties for the Twitter driver.	
Authentication Mode	The authentication mode that the Twitter driver must use. Valid values are OAuth and xAuth.	OAuth
Username	The user name of the Twitter user.	MrSmith
Password	The password of the Twitter user.	password
ConsumerKey	The public key of the Twitter user.	Kr7px6Kav0ph0GLHQxa91W
ConsumerSecret	The private key of the Twitter user.	ezDK6Ky9tIBxqMDIAPm752nFzIBdqqJF5Q4G9Bzotu
Access Token	The public key of a registered Twitter application.	1091745185-SVKsxv7PFsBrFgSrywnqylWp3ANr8as9QRMohnj
Access Token Secret	The private key of a registered Twitter application.	Q1PcWeDTVhaKH3DhJ9i1klosXAtfXwXR257JEiqeYu

[Table A–23](#) describes the move plan properties that you can change for Oracle B2B. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment.

Table A–23 Move Plan Properties for Oracle B2B

Property	Description	Sample Value
Property in the B2B System Parameters configGroup:	B2B system parameter configuration.	
Callout Directory	The absolute path of the Callout directory.	/tmp/calloutDirectory
Large Payload Directory	The absolute path of the large payload directory.	/tmp
SMTP Host	The host name of the SMTP server in the enterprise to send the negative MDN to the trading partner for an ASI exchange.	host.example.com
Webservice policy	The URI for the security policy used to secure the Web service.	oracle/wss_username_token_service_policy

Table A-23 (Cont.) Move Plan Properties for Oracle B2B

Property	Description	Sample Value
SSL Private Key Password	The absolute path of a secure file containing the password. If a password file is not provided, the value will not be set in target.	/tmp/passwordfile/sslpwd.txt
<hr/>		
Property in the File.DeliveryChannel configGroup:	File Delivery Channel configuration.	
file-param-folder	The absolute path of the folder.	/tmp/file_deliv
Property in the File.ListeningChannel configGroup:	File Listening Channel configuration.	
file-param-folder	The absolute path of the folder.	/tmp/file_listen
Properties in the JMS configGroup:	JMS configuration. Each channel has its own set of property values.	
jms-param-password	The absolute path of a secure file containing the password. If a password file is not provided, the value will not be set in target. The source configuration will be retained.	/tmp/password/pass.txt
jms-param-is_topic	A flag specifying whether or not this is a configured destination topic. Valid values are true and false.	false
jms-param-queue_name	The JNDI name of the queue or topic.	jms/b2b/B2B_IN_QUEUE
jms-param-DestinationProviderProperties	The JMS destination provider properties. Use a semicolon (;) as the separator for each key/value pair.	java.naming.provider.url=t3://example.com:7001; java.naming.factory.initial=weblogic.jndi.WLInitialContextFactory; java.naming.security.principal=weblogic; java.naming.security.credentials=weblogic Enter this on one line.
jms-param-user	The JMS user name.	user1
Properties in the FTP configGroup:	FTP configuration. Each channel has its own set of property values.	
ftp-param-password	The absolute path of a secure file containing the password. If a password file is not provided, the value will not be set in target. The source configuration will be retained.	/tmp/password/pass.txt
ftp-param-folder	The absolute path of the folder.	/tmp/test1
ftp-param-host	The FTP host name.	example
ftp-param-preserve_filename	A flag that specifies whether the file name will be preserved. Valid values are true and false.	false
ftp-param-user	The FTP user name.	User

Table A–23 (Cont.) Move Plan Properties for Oracle B2B

Property	Description	Sample Value
Properties in the HTTP configGroup:	HTTP configuration. Each channel has its own set of property values.	
http-param-password	The absolute path of a secure file containing the password. If a password file is not provided, the value will not be set in target. The source configuration will be retained.	/tmp/password/pass.txt
http-param-use_proxy	A flag that specifies whether to use a proxy server. Valid values are true and false.	false
http-param-additional_headers	Additional transport headers, for example, headers for digest authentication.	
http-param-url	The fully qualified HTTP URL.	http://example:8001/b2b/httpReceiver
as2-param-Receipt-Delivery-Option	The fully qualified HTTP URL.	http://example:8001/b2b/httpReceiver
Properties for the SFTP transport protocol:	The SFTP configuration.	
sftp-param-password	The absolute path of a secure file containing the password. If a password file is not provided, the value will not be set in target. The source configuration will be retained.	/tmp/password/pass.txt
sftp-param-host	The SFTP host name.	example
sftp-param-port	The SFTP port number.	22
sftp-param-folder	The absolute path of the folder.	/scratch/b2b/sftp
sftp-param-user	The name of the SFTP user.	user1
Properties for the Email transport protocol:	The email configuration.	
email-param-password	The absolute path of a secure file containing the password. If a password file is not provided, the value will not be set in target. The source configuration will be retained.	/tmp/password/pass.txt
email-param-host	The email host name.	example
email-param-user	The email user name.	user1
email-param-email-id	The email address to which messages are delivered (similar to specifying the path for a file channel or queues in AQ or JMS).	user1@exampleb2b.com
Properties for the AQ transport protocol:	The AQ configuration.	
aq-param-password	The absolute path of a secure file containing the password. If a password file is not provided, the value will not be set in target. The source configuration will be retained.	/tmp/password/pass.txt
aq-param-datasource	The JNDI name of the JDBC data source to access AQ queues.	jdbc/SOADatasource

Table A–23 (Cont.) Move Plan Properties for Oracle B2B

Property	Description	Sample Value
aq-param-recipient	The value used when delivering a message to the AQ queue.	testuser
aq-param-queue_name	The AQ queue name.	IP_OUT_QUEUE
aq-param-consumer	The client that receives the message.	b2buser
Properties for the TCP transport protocol:	The TCP configuration.	
tcp-param-host	The TCP host name.	example
tcp-param-port	The TCP port number.	23456
tcp-param-PermanentConnectionType	A flag indicating whether or not a cached connection is used to exchange all the messages. Valid values are true and false.	false
tcp-param-timeout	The TCP timeout, in seconds.	300

Table A–24 describes the move plan properties that you can change for Oracle Enterprise Scheduler. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment. The move plan can also contain properties that you have defined in your source environment. Modify any READ_WRITE properties with values that are valid for the target environment.

Table A–24 Move Plan Properties for Oracle Enterprise Scheduler

Property	Description	Sample Value
Properties in the ESS_CONFIG_XML configGroup:	Configuration properties for Oracle Enterprise Scheduler	
RequestFileDirectory	The directory for request and log output.	/tmp/ess/RequestFileDirectory
RequestFileDirectoryShared	A flag indicating whether the request file directory is shared. Valid values are true or false. The default is false.	false
Properties in the ESS_ADF_DOMAIN_CONFIG configGroup:	Properties configured in adf-domain-config.xml, to assist Oracle Enterprise Scheduler request output and post processing.	
essappFilePersistenceMode	The file persistence mode for storing the output of request execution.	file
essappRequestFileDirectory	The directory for request and log output for the Oracle Enterprise Scheduler application.	/tmp/ess/MyRFD
essappCallbackClientSecurityPolicyURI	The security policy URI used in the WS-Security headers for web service invocations from Oracle Enterprise Scheduler for web service callbacks.	oracle/wss11_saml_token_with_message_protection_client_policy
umsAppInternalHost	The UMS Server NotificationServiceURL host name.	example.domain.com
umsAppInternalPort	The UMS Server NotificationServiceURL port.	10999
umsAppInternalProtocol	The UMS Server NotificationServiceURL protocol.	http
ucmAppInternalSamlTokenPolicyURI	The SAML Policy URI.	

Table A-25 describes the move plan properties that you can change for Oracle Managed File Transfer. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment.

Table A-25 Move Plan Properties for Oracle Managed File Transfer

Property	Description	Sample Value
Properties in the MFT System Properties configGroup:	The system properties configuration	
Server Properties	Server properties	
Payload Storage Directory	The full path to file system location where files being transferred are stored.	/scratch/oracle/mft/storage
Callout Directory	The location where custom callouts are stored.	/scratch/oracle/mft/callouts
External Address	The external IP address or host name of the load balancer. If the load balancer is not being used, then it can refer to any external address with which payload references can be sent to customers.	host.example.com
Internal Address	The internal IP address or host name of the load balancer. If the load balancer is not being used, then it can refer to any internal address with which payload references can be sent to customers.	host.example.com
KeyStore Properties	The keystore properties	
Default Keystore Password File	The absolute path of a secure file that contains the password for the default keystore.	/scratch/oracle/t2p/mft_db_pass.txt
Default Keystore Private Key Password File	The absolute path of a secure file that contains the password for the default keystore private key.	/scratch/oracle/t2p/mft_pvt_pass.txt
SSH Keystore Private Key Password File	The absolute path of a secure file that contains the password for the SSH keystore private key.	/scratch/oracle/t2p/mft_ssh_pass.txt
PGP Keystore Private Key Password File	The absolute path of a secure file that contains the password for the PGP keystore private key.	/scratch/oracle/t2p/mft_pgp_pass.txt
Embedded Server Properties	Properties for embedded FTP and sFTP servers.	
Embedded Server Root Directory	The root directory location for the embedded FTP and sFTP servers.	\$DOMAIN_HOME/mft/ftp_root
Domains Properties	The configuration properties for the domain.	
Domain Alias	The alias for the domain. It is used to refer to the domain details while configuring the source or target.	B2B Remote
Connection URL	The URL for connecting to the domain.	t3://localhost:7001
User Name	The user name for the domain.	weblogic

Table A–25 (Cont.) Move Plan Properties for Oracle Managed File Transfer

Property	Description	Sample Value
Password File	The absolute path of a secure file that contains the password for the domain.	/scratch/oracle/t2p/mft_dom_pass.txt
Type	The domain type: B2B, Healthcare, SOA, Service Bus, or ODI.	B2B

Table A–26 describes the move plan properties that you can change for Oracle Data Integrator. Edit all properties, such as host names, port numbers, listen addresses, that have different values in the target environment.

Table A–26 Move Plan Properties for Oracle Data Integrator

Property	Description	Sample Value
Properties in the Master Repository configGroup:	Master repository configuration	
Url	JDBC URL for connecting to the master repository.	jdbc:oracle:thin:@localhost:1522:orc1
Schema name	The name of the schema in the target database where the target ODI repository will be created.	odi_master_12c
Schema password file	The absolute path of a secure file that contains the password for the schema.	/scratch/oracle/odi_schema_passwd.txt
SUPERVISOR user	The name of the ODI user SUPERVISOR.	SUPERVISOR
SUPERVISOR password file	The absolute path of a secure file that contains the password for the ODI user SUPERVISOR.	/scratch/oracle/odi_passwd.txt
Properties in the Physical Data Servers configProperty:	Data servers configuration	
Schema name	The name of the schema for the database data servers or the directory location for file type data servers.	FG_Dir_Schema
Work Schema	The name of the Work schema for the database data servers or the directory location for file type data servers.	/tmp/FG_Dir_Schema
Url	JDBC URL for connecting to the data server.	jdbc:oracle:thin:@localhost:1521/example.com
User	User name for the physical data servers connection.	username
Password File	The absolute path of a secure file that contains the password for the user for the physical data servers connection.	/scratch/oracle/rpd_ds_conn_passwd.txt
Properties in the Agents configProperty:	Agents configuration	
Host name	The Agent host name.	localhost
Host port	The Agent host port number.	12311
Properties in the Work Repositories configProperty:	Work repositories configuration	

Table A–26 (Cont.) Move Plan Properties for Oracle Data Integrator

Property	Description	Sample Value
Url	JDBC URL for connecting to the work repository.	jdbc:oracle:thin:@localhost:1521/example.com
User	User name for connecting to the work repository.	username
Password File	The absolute path of a secure file that contains the password for the user for the physical data servers connection.	/scratch/oracle/odi_pds_passwd.txt

B

Oracle Fusion Middleware Command-Line Tools

This appendix summarizes the command-line tools that are available in Oracle Fusion Middleware.

Table B-1 Oracle Fusion Middleware Command-Line Tools

Command	Path	Description
adrci	UNIX: <i>ORACLE_HOME</i> /oracle_common/adr/adcri.sh Windows: <i>ORACLE_HOME</i> \oracle_common\adr\adrci.bat	Package incident and problem information into a zip file for transmission to Oracle Support.
config	UNIX: <i>ORACLE_HOME</i> /oracle_common/common/bin/config.sh Windows: <i>ORACLE_HOME</i> \oracle_common\common\bin\config.cmd	Invoke the Configuration Wizard to create and configure a domain or extend a domain. See: The Installation Guide for the component.
ua	UNIX: <i>ORACLE_HOME</i> /oracle_common/upgrade/bin /ua Windows: <i>ORACLE_HOME</i> \oracle_common\upgrade\ua.bat	Oracle Fusion Middleware Upgrade Assistant. See: <i>Planning an Upgrade of Oracle Fusion Middleware</i>
orapki	UNIX: <i>ORACLE_HOME</i> /oracle_common/bin/orapki Windows: <i>ORACLE_HOME</i> \oracle_common\bin\orapki.bat	Manages wallets and certificates. See Appendix G .
wlst	UNIX: <i>ORACLE_HOME</i> /oracle_common/common/bin/wlst.sh Windows: <i>ORACLE_HOME</i> \oracle_common\common\bin\wlst.cmd	(WebLogic Scripting tool) Manages Oracle WebLogic Server and the components in an Oracle WebLogic Server domain. See: Section 2.4, WLST Command Reference for WebLogic Server , and WLST Command Reference for Infrastructure Components

URLs for Components

This appendix provides the URLs needed to access Oracle Fusion Middleware components.

[Table C-1](#) shows the URLs to access components after installation.

The URLs in the table are shown with the default ports. The components in your environment might use different ports. To determine the port numbers, from the WebLogic Domain menu in Fusion Middleware Control, select **Port Usage**.

Table C-1 *URLs for Components*

Component	URL (with Default Port Number)
Oracle B2B	http://host:8001/b2b
Oracle Business Activity Monitoring	http://host:9001/oracleBAM
Oracle Enterprise Manager Fusion Middleware Control	http://host:7001/em
Oracle HTTP Server	http://host:7777
Oracle Managed File Transfer	http://host:7001/mftconsole
Oracle Service Bus	http://host:7001/sbconsole
Oracle WebLogic Server Administration Console	http://host:7001/console

Port Numbers

This appendix provides information about Oracle Fusion Middleware port numbers. It contains the following sections:

- [Section D.1, "Port Numbers by Component"](#)
- [Section D.2, "Port Numbers \(Sorted by Number\)"](#)

D.1 Port Numbers by Component

This section provides the following information for each Oracle Fusion Middleware component or service that uses a port:

- **Component or Service:** The name of the component and service.
- **Default Port Number:** The first port number Oracle Fusion Middleware attempts to assign to a component. It is usually the lowest number in the allotted port range. If the port is in use, the next available port number, within the allotted range, is assigned.
- **Allotted Port Range:** The set of port numbers Oracle Fusion Middleware attempts to use when assigning a port.

Port numbers for Oracle WebLogic Server servers are assigned sequentially for each server created. For example, the first Administration Server is assigned the port 7001, the second 7002. Managed Servers created during installation and configuration for particular components may have specific default port numbers.

[Table D-1](#) shows the default port number and the port number range for components, sorted alphabetically by component.

Table D-1 Port Numbers Sorted by Component

Component or Service	Default Port Number	Allotted Port Range
Oracle Business Activity Monitoring	9001	9000-9080
Oracle Data Integrator	15000	15500
Oracle HTTP Server non-SSL Listen Port	7777 or 8888	7777-7877, 8888
Oracle HTTP Server SSL Listen Port	4443	4443-4543
Oracle WebLogic Server Listen Port for Administration Server	7001	7001-9000
Oracle WebLogic Server Listen Port for Managed Server	8001	8000 - 8080

Table D-1 (Cont.) Port Numbers Sorted by Component

Component or Service	Default Port Number	Allotted Port Range
Oracle WebLogic Server Node Manager Port	5556	5556
Oracle WebLogic Server SSL Listen Port for Administration Server	7002	7002-9000

D.2 Port Numbers (Sorted by Number)

[Table D-2](#) lists Oracle Fusion Middleware ports numbers and components, sorted in ascending order by port number.

Table D-2 Port Numbers Sorted by Number

Default Port Number	Component or Service
4443	Oracle HTTP Server (SSL)
5556	Oracle WebLogic Server Node Manager Port
7001	Oracle WebLogic Server Listen Port for Administration Server
7002	Oracle WebLogic Server SSL Listen Port for Administration Server
7777	Oracle HTTP Server (non-SSL)
9001	Oracle Business Activity Monitoring Managed Server
15000	Oracle Data Integrator

Using Oracle Fusion Middleware Accessibility Options

This appendix includes information about using Oracle Fusion Middleware accessibility options.

It includes the following sections:

- [Section E.1, "Install and Configure Java Access Bridge \(Windows Only\)"](#)
- [Section E.2, "Enabling Fusion Middleware Control Accessibility Mode"](#)
- [Section E.3, "Fusion Middleware Control Keyboard Navigation"](#)

E.1 Install and Configure Java Access Bridge (Windows Only)

If you are installing on a Windows computer, you can install and configure Java Access Bridge for Section 508 Accessibility:

1. Download Java Access Bridge from the following URL:
<http://www.oracle.com/technetwork/java/javase/tech/index-jsp-136191.html>
2. Install Java Access Bridge.
3. Copy the `access-bridge.jar` and `jaccess-1_4.jar` files from your installation location to the `jre/lib/ext` directory.
4. Copy the `WindowsAccessBridge.dll`, `JavaAccessBridge.dll`, and `JAWTAccessBridge.dll` files from your installation location to the `jre/bin` directory.
5. Copy the `accessibility.properties` file to the `jre/lib` directory.

E.2 Enabling Fusion Middleware Control Accessibility Mode

The following sections provide information on the benefits of running Fusion Middleware Control in accessibility mode, as well as instructions for enabling accessibility mode:

- [Making HTML Pages More Accessible](#)
- [Viewing Text Descriptions of Fusion Middleware Control Charts](#)

E.2.1 Making HTML Pages More Accessible

In Fusion Middleware Control, you can enable screen reader support. Screen reader support improves behavior with a screen reader. This is accomplished by adding accessibility-specific constructs to the HTML, and by altering some navigation elements on the pages.

To enable screen reader mode in Fusion Middleware Control:

1. Choose the user name at the right top of the page, then **Accessibility**.
The Accessibility Preference page is displayed.
2. Select any of the following options:
 - **I use a screen reader:** Accessibility-specific constructs are added to improve behavior with a screen reader.
 - **I use high contrast settings:** The fonts use a high contrast.
 - **I use large fonts:** The fonts are larger than normal.
 - **Show me the Accessibility Preference dialog when I log in:** When you log in, the Accessibility Preference page is displayed.
3. Click **Apply**.
A confirmation dialog box is displayed.
4. Click **OK**.
5. Click Enterprise Manager at the top of the page to return to the page you last visited.

When you select screen reader support, Fusion Middleware Control renders the Web pages so that they can be read by a screen reader. For example, each node in the navigation tree includes a Select button.

The following figure shows the navigation pane and the Administration Server Performance Summary after enabling screen reader support:

The screenshot displays the Fusion Middleware Control interface for a WebLogic Domain. The interface is divided into several sections:

- Change Center:** Shows 'Changes' and 'Recording' options.
- Target Navigation:** A tree view on the left showing the hierarchy: Application Deployments > SOA > WebLogic Domain > soa_domain. Under 'soa_domain', various servers and clusters are listed, including AdminServer, bam_server1, ess_server1, mft_server1, osb_server1, soa_cluster_1, and ums_server1.
- Summary:** Provides general information about the domain:
 - Administration Server: AdminServer
 - Administration Server Host: slc01fkr.us.oracle.com
 - Administration Server Listen Port: 7001
 - Support Workbench Problems: 0
- Tools:** A link to the WebLogic Server Administration Console.
- Servers:** A table showing server status:

Series	Group	Target Count	Data Type	Value	Percent
Down (5)		5			62%
Up (3)		3			38%
- Clusters:** A table showing cluster status:

Name	Servers	Clus Add
Oracle WebLogic Cluster soa_cluster_1	2	
- Deployments:** A table showing deployment status:

Series	Group	Target Count	Data Type	Value	Percent
Down (105)		105			51%
Up (101)		101			49%

E.2.2 Viewing Text Descriptions of Fusion Middleware Control Charts

Throughout Fusion Middleware Control, charts are used to display performance data. For most users, these charts provide a valuable graphical view of the data that can reveal trends and help identify minimum and maximum values for performance metrics.

However, charts do not convey information in a manner that can be read by a screen reader. To remedy this problem, you can configure Fusion Middleware Control to provide a complete textual representation of each performance chart. When you enable screen reader mode, Fusion Middleware Control displays the information in tables, instead of charts.

To view a representation of the data in a table, instead of a chart, without enabling screen reader mode, click **Table View** below a chart.

E.3 Fusion Middleware Control Keyboard Navigation

This section describes the keyboard navigation in Fusion Middleware Control.

Much of the keyboard navigation is the same whether or not you use screen reader mode.

Generally, you use the following keys to navigate:

- **Tab key:** Move to the next control, such as a dynamic target menu, navigation tree, content pane, or tab in a page. Tab traverses the page left to right, top to bottom. Use Shift + Tab to move to the previous control.
- **Up and Down Arrow keys:** Move to the previous or next item in the navigation tree, menu, or table. Down Arrow also opens a menu.

- Left and Right Arrow keys: Collapse and expand an item in the navigation tree or a submenu.
- Esc: Close a menu.
- Spacebar: Activate a control. For example, in a check box, spacebar toggles the state, checking or unchecking the box. On a link, spacebar navigates to the target of the link.
- Enter: Activate a button.

Table E-1 shows some common tasks and the keyboard navigation used.

Table E-1 Keyboard Navigation for Common Tasks

Task	Navigation
Move to next control, such as navigation tree or menu	Tab
Move to previous control, such as navigation tree or menu	Shift+Tab
Move to navigation pane	Tab until navigation tree has input focus
Move down the navigation tree	Down Arrow
Move up the navigation tree	Up Arrow
Expand a folder	Right Arrow
Collapse a folder	Left Arrow
Open a menu	Down Arrow
Move to the next item in a menu	Down Arrow
Move to the previous item in a menu	Up Arrow
Select a menu item	Enter
Open a submenu	Right Arrow
Close a submenu	Left Arrow
Move out of a menu	Esc
Activate a button	Enter
Open a tab in a content pane	Tab to the content pane, Tab to the tab to get input focus, then Enter to select the tab
Select an item, such as Message type in Log Messages screen	Spacebar
Select a row in a table	Tab to the header of the table, then Down Arrow to move to a row
Select a cell in a table	Tab to the header of the table, then Tab until you reach the cell you want to select, then Enter

Table E-2 shows the keyboard navigation for the Topology Viewer. The navigation from one node to another is based on the geometry of the topology.

Table E-2 Keyboard Navigation for Topology Viewer

Task	Navigation
Navigate into the topology	Tab, until you have reached a node.

Table E-2 (Cont.) Keyboard Navigation for Topology Viewer

Task	Navigation
Navigate nodes based on geometry	Arrow keys
In a top-to-bottom orientation, navigate to a destination link	Ctrl+Shift+Down Arrow
In a top-to-bottom orientation, navigate to a source link	Ctrl+Shift+Up Arrow
In a left-to-right orientation, navigate to a destination link	Ctrl+Shift+Right Arrow
In a left-to-right orientation, navigate to a source link	Ctrl+Shift+Left Arrow
In a top-down orientation, when on a link, navigate to other links. The focus moves to another link based on the geometry.	Right Arrow or Left Arrow
In a left-to-right orientation, when on a link, navigate to other links. The focus moves to another link based on the geometry.	Up Arrow or Down Arrow
Move into or out of a group node	Shift+Arrow
Simulate a mouse click on the node. This can bring up a popup or it can navigate to another page.	Enter
Simulate a mouse over. Typically, this brings up a popup.	Shift+Enter
Simulate a right-mouse click. Typically, this brings up a context menu.	m
Expand or contract a node subtree	e
Expand or contract a group. Note that if you use Shift+Arrow to move into a group, the group automatically expands.	g
Pan up or down, left or right	Ctrl+Arrow keys
Zoom in	Ctrl+Alt+Plus Key(+)
Zoom out	Ctrl+Alt+Minus Key(-)
Move out of a menu.	Esc

Viewing Release Numbers

This appendix describes how to view Oracle Fusion Middleware release numbers.

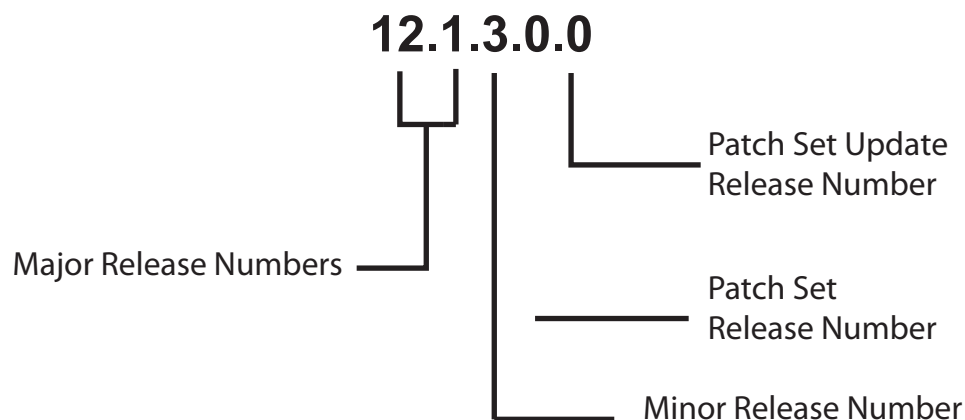
It appendix contains the following sections:

- [Section F.1, "Release Number Format"](#)
- [Section F.2, "Viewing the Software Inventory and Release Numbers"](#)

F.1 Release Number Format

To understand the release level nomenclature used by Oracle, examine the example of an Oracle Fusion Middleware release number shown in [Figure F-1](#).

Figure F-1 Example of an Oracle Fusion Middleware Release Number



In [Figure F-1](#), each digit is labeled:

- The first two numbers are the Major Release number.
This is the most general identifier. It represents a major new edition (or version) of Oracle Fusion Middleware, and indicates that the release contains significant new functionality.
- The third number is the Minor release number.
- The fourth number indicates a Patch Set release.
- The fifth number indicates a Patch Set Update release.

F.2 Viewing the Software Inventory and Release Numbers

The following sections describe how to obtain the release numbers of Oracle Fusion Middleware:

- [Viewing Oracle Fusion Middleware Installation Release Numbers](#)
- [Viewing Component Release Numbers](#)
- [Viewing Metadata Repository Release Numbers](#)

F.2.1 Viewing Oracle Fusion Middleware Installation Release Numbers

All Oracle Fusion Middleware installations have a release number. This number is updated when you apply a patch set release or upgrade the installation.

You can view the release number of an Oracle Fusion Middleware installation using OPatch. Run the following command:

```
(UNIX) ORACLE_HOME/OPatch/opatch lsinventory
(Windows) ORACLE_HOME\OPatch\opatch lsinventory
```

For example, on UNIX:

```
./opatch lsinventory
Copyright (c) 2014, Oracle Corporation. All rights reserved.

Oracle Home      : /scratch/oracle1/Oracle/Middleware/Oracle_Home
Central Inventory : /scratch/oracle1/oraInventory
  from           : /scratch/oracle1/Oracle/Middleware/Oracle_Home/oraInst.loc
OPatch version   : 13.2.0.0.0
OUI version      : 13.2.0.0.0
Log file location : /scratch/oracle1/Oracle/Middleware/Oracle_
Home/cfgtoollogs/opatch/opatch2014-05-29_13-23-02PM_1.log

OPatch detects the Middleware Home as "/scratch/oracle1/Oracle/Middleware/Oracle_
Home"
May 29, 2014 1:23:33 PM oracle.sysman.oii.oi.iii.OiiiInstallAreaControl
initAreaControl
INFO: Install area Control created with access level 0
Lsinventory Output file location : /scratch/oracle1/Oracle/Middleware/Oracle_
Home/cfgtoollogs/opatch/lsinv/lsinventory2014-05-29_13-23-02PM.txt

-----

There are no Interim patches installed in this Oracle Home.
```

F.2.2 Viewing Oracle WebLogic Server Release Numbers

You can use the following command to view the release number of Oracle WebLogic Server:

```
(UNIX) cat $ORACLE_HOME/wlserver/.product.properties | grep WLS_PRODUCT_VERSION
(Windows) type %ORACLE_HOME%\wlserver\.product.properties | findstr WLS_PRODUCT_
VERSION
```

For example, on UNIX:

```
cat $ORACLE_HOME/wlserver/.product.properties | grep WLS_PRODUCT_VERSION
WLS_PRODUCT_VERSION=12.1.3.0.00
```


F.2.3 Viewing Component Release Numbers

All Oracle Fusion Middleware components have a release number and many contain services that have release numbers. These numbers *may* be updated when you apply a patch set release or upgrade the installation.

You can view the release number of components and their services by using the following commands:

- On UNIX:

```
cd ORACLE_HOME/inventory
ls -d Components*/**/*
```

- On Windows:

```
cd ORACLE_HOME/inventory/Componentsn
dir /S /A:D
```

F.2.4 Viewing Metadata Repository Release Numbers

If you are using an Oracle Database instance for your metadata repository, you can view the release number of the database using SQL*Plus as follows (you can be connected to the database as any user to issue these commands):

```
SQL> COL PRODUCT FORMAT A40
SQL> COL VERSION FORMAT A15
SQL> COL STATUS FORMAT A15
SQL> SELECT * FROM PRODUCT_COMPONENT_VERSION;
```

PRODUCT	VERSION	STATUS
-----	-----	-----
NLSRTL	11.2.0.4.0	Production
Oracle Database 11g Enterprise Edition	11.2.0.4.0	Production
PL/SQL	11.2.0.4.0	Production
TNS for Linux:	11.2.0.4.0	Production

F.2.5 Viewing Schema Release Numbers

If you are using an Oracle Database instance for your metadata repository, you can view the release number of the schema using SQL*Plus, as follows:

```
SQL> COL COMP_ID FORMAT A20
SQL> COL COMP_NAME A40
SQL> COL VERSION FORMAT A20
SQL> SELECT COMP_ID, COMP_NAME, VERSION FROM SCHEMA_VERSION_REGISTRY;
```

COMP_ID	COMP_NAME	VERSION
-----	-----	-----
.		
.		
.		
MDS	Metadata Services	12.1.3.0.0
OPSS	Oracle Platform Security Services	12.1.3.0.0
SOAINFRA	SOA Infrastructure Services	12.1.3.0.0
STB	Service Table	12.1.3.0.0
.		
.		
.		

Use this appendix to learn about how to transition from pre-12c tools like `orapki` to the certificate, wallet management, and SSL configuration tools provided in 12c (12.1.3).

Oracle Application Server 10g provided the `orapki` utility, a command-line tool to manage certificate revocation lists (CRLs), create and manage Oracle wallets, and create signed certificates for testing purposes. It also provided the SSL Configuration Tool.

Oracle Fusion Middleware 12c (12.1.3) provides both command-line and graphical user interfaces to configure SSL. The Oracle WebLogic Scripting Tool (WLST) and Oracle Enterprise Manager Fusion Middleware Control enable you to manage KSS- and JKS-based keystores, wallets, and certificates.

The appendix contains the following section:

- [Section G.1, "Using the orapki Utility for Certificate and CRL Management"](#)

See Also:

- Doc ID 1629906.1 "How To Create a Wallet via ORAPKI in Fusion Middleware 12c" in the Oracle Technology Network Knowledge Base for additional information and examples of the `orapki` commands shown in this appendix.
- *Infrastructure Security WLST Command Reference* for examples of the WLST commands shown in this appendix.
- [Chapter 6](#) for details about keystore and wallet management in Oracle Fusion Middleware.

Note: The `orapki` utility is located in the binary directory of Oracle Common home, that is, `$ORACLE_HOME/oracle_common/bin`.

G.1 Using the `orapki` Utility for Certificate and CRL Management

This section contains these topics:

- [orapki Overview](#)
- [Displaying orapki Help](#)
- [Creating Signed Certificates for Testing Purposes](#)
- [Managing Oracle Wallets with the orapki Utility](#)

- [Managing Certificate Revocation Lists \(CRLs\) with orapki Utility](#)
- [orapki Utility Commands Summary](#)

G.1.1 orapki Overview

The `orapki` utility is provided to manage public key infrastructure (PKI) elements, such as wallets and certificate revocation lists, on the command line so the tasks it performs can be incorporated into scripts. This enables you to automate many of the routine tasks of maintaining a PKI.

This command-line utility can be used to perform the following tasks:

- Creating signed certificates for testing purposes
- Managing Oracle wallets:
 - Creating and displaying Oracle wallets
 - Adding and removing certificate requests
 - Adding and removing certificates
 - Adding and removing trusted certificates
- Managing certificate revocation lists (CRLs):
 - Renaming CRLs with a hash value for certificate validation

`orapki` allows you to import certificates in both DER and PEM formats.

G.1.1.1 orapki Syntax

The basic syntax of the `orapki` command-line utility is as follows:

```
orapki module command -parameter value
```

In the preceding command, *module* can be `wallet` (Oracle wallet), `crl` (certificate revocation list), or `cert` (PKI digital certificate). The available commands depend on the *module* you are using. For example, if you are working with a `wallet`, then you can add a certificate or a key to the wallet with the `add` command. The following example adds the user certificate located at `/private/lhale/cert.txt` to the wallet located at `ORACLE_HOME/wallet/ewallet.p12`:

```
orapki wallet add -wallet ORACLE_HOME/wallet/ewallet.p12  
-user_cert -cert /private/lhale/cert.txt
```

DN Syntax is Platform-specific

Many `orapki` commands require the specification of the DN. On UNIX, the `user_dn` is surrounded by single quotes, for example:

```
ORACLE_HOME/oracle_common/bin/orapki wallet add  
-wallet ORACLE_HOME/wallet  
-dn 'CN=server.in.oracle.com, OU=Support, O=Oracle, L=Jaipur, ST=Rajasthan, C=IN'  
-keysize 1024
```

Windows requires double quotes:

```
ORACLE_HOME/oracle_common/bin/orapki wallet add  
-wallet ORACLE_HOME/wallet  
-dn "CN=server.in.oracle.com, OU=Support, O=Oracle, L=Jaipur, ST=Rajasthan, C=IN"  
-keysize 1024
```

G.1.1.2 Environment Setup for orapki

When running orapki in the context of Web Tier installations, set ORACLE_HOME to point to the product installation location.

G.1.2 Displaying orapki Help

You can display all the orapki commands that are available for a specific mode by entering the following at the command line:

```
orapki mode help
```

For example, to display all available commands for managing certificate revocation lists (CRLs), enter the following at the command line:

```
orapki crl help
```

Note: Using the `-summary`, `-complete`, or `-wallet` command options is always optional. A command will still run if these command options are not specified.

G.1.3 Creating Signed Certificates for Testing Purposes

This command-line utility provides a convenient, lightweight way to create signed certificates for testing purposes. The following syntax can be used to create signed certificates and to view certificates:

To create a signed certificate for testing purposes:

```
orapki cert create [-wallet wallet_location] -request
  certificate_request_location
  -cert certificate_location -validity number_of_days [-summary]
```

This command creates a signed certificate from the certificate request. The `-wallet` parameter specifies the wallet containing the user certificate and private key that will be used to sign the certificate request. The `-validity` parameter specifies the number of days, starting from the current date, that this certificate will be valid. Specifying a certificate and certificate request is mandatory for this command.

To view a certificate:

```
orapki cert display -cert certificate_location [-summary | -complete]
```

This command enables you to view a test certificate that you have created with orapki. You can choose either `-summary` or `-complete`, which determines how much detail the command will display. If you choose `-summary`, the command will display the certificate and its expiration date. If you choose `-complete`, it will display additional certificate information, including the serial number and public key.

G.1.4 Managing Oracle Wallets with the orapki Utility

The following sections describe the syntax used to create and manage Oracle wallets with the orapki command-line utility. You can use these orapki utility wallet module commands in scripts to automate the wallet creation process.

- [Creating and Viewing Oracle Wallets with orapki](#)
- [Adding Certificates and Certificate Requests to Oracle Wallets with orapki](#)
- [Exporting Certificates and Certificate Requests from Oracle Wallets with orapki](#)

Note: The `-wallet` parameter is mandatory for all `wallet` module commands.

See Also: For examples of how to create either a password-protected wallet or an auto-login wallet, see Doc ID 1629906.1 "How To Create a Wallet via ORAPKI in Fusion Middleware 12c" on the Oracle Technology Network Knowledge Base.

- [Creating and Managing Trust Flags](#)
- [Importing PKCS#12 Files to an Oracle Wallet](#)

G.1.4.1 Creating and Viewing Oracle Wallets with orapki

This section contains these topics:

- [Creating an Oracle Wallet](#)
- [Creating an Oracle Wallet with Auto-login Enabled](#)
- [Creating an Oracle Wallet with AES Encryption](#)
- [Converting an Existing Wallet to Use AES Encryption](#)
- [Viewing an Oracle Wallet](#)

G.1.4.1.1 Creating an Oracle Wallet

```
orapki wallet create -wallet wallet_location
```

This command prompts you to enter and re-enter a wallet password. It creates a wallet in the location specified for `-wallet`.

G.1.4.1.2 Creating an Oracle Wallet with Auto-login Enabled

```
orapki wallet create -wallet wallet_location -auto_login
```

This command creates a wallet with auto-login enabled. It can also be used to enable auto-login on an existing wallet. If the `wallet_location` already contains a wallet, then auto-login will be enabled for it. To disable the auto-login feature, delete `cwallet.sso`.

Note: For wallets with the auto-login feature enabled, you are prompted for a password only for operations that modify the wallet, such as `add`.

G.1.4.1.3 Creating an Oracle Wallet with AES Encryption

```
orapki wallet create -wallet wallet -pwd pwd -compat_v12
```

This command creates an Oracle wallet with AES encryption.

G.1.4.1.4 Converting an Existing Wallet to Use AES Encryption

```
orapki wallet convert -wallet wallet -compat_v12 -pwd pwd
```

This command converts an Oracle wallet from 3DES to AES encryption.

G.1.4.1.5 Viewing an Oracle Wallet

```
orapki wallet display -wallet wallet_location
```

This command displays the certificate requests, user certificates, and trusted certificates contained in the wallet.

G.1.4.2 Adding Certificates and Certificate Requests to Oracle Wallets with orapki

This section contains these topics:

- [Adding a Certificate Request to an Oracle Wallet](#)
- [Adding a Trusted Certificate to an Oracle Wallet](#)
- [Adding a Root Certificate to an Oracle Wallet](#)
- [Adding a User Certificate to an Oracle Wallet](#)

G.1.4.2.1 Adding a Certificate Request to an Oracle Wallet

```
orapki wallet add -wallet wallet_location -dn user_dn -keysize 512|1024|2048|4096
```

This command adds a certificate request to a wallet for the user with the specified distinguished name (*user_dn*). The request also specifies the requested certificate's key size (512, 1024, or 2048 bits). To sign the request, export it with the export option. See [Section G.1.4.3, "Exporting Certificates and Certificate Requests from Oracle Wallets with orapki."](#)

For example:

Linux/Unix:

```
$ORACLE_HOME/oracle_common/bin/orapki wallet add
-wallet $ORACLE_HOME/wallet
-dn 'CN=server.in.test.com, OU=Support, O=Oracle, L=Jaipur, ST=Rajasthan, C=IN'
-keysize 1024
```

Windows:

```
$ORACLE_HOME/oracle_common/bin/orapki wallet add
-wallet $ORACLE_HOME/wallet
-dn "CN=server.in.test.com, OU=Support, O=Oracle, L=Jaipur, ST=Rajasthan, C=IN"
-keysize 1024
```

G.1.4.2.2 Adding a Trusted Certificate to an Oracle Wallet

```
orapki wallet add -wallet wallet_location -trusted_cert -cert
certificate_location
```

This command adds a trusted certificate, at the specified location (*-cert certificate_location*), to a wallet. You must add all trusted certificates in the certificate chain of a user certificate before adding a user certificate, or the command to add the user certificate will fail.

G.1.4.2.3 Adding a Root Certificate to an Oracle Wallet

```
orapki wallet add -wallet wallet_location -dn
certificate_dn -keysize 512|1024|2048 -self_signed -validity number_of_days
```

This command creates a new self-signed (root) certificate and adds it to the wallet. The *-validity* parameter (mandatory) specifies the number of days, starting from the current date, that this certificate will be valid. You can specify a key size for this root certificate (*-keysize*) of 512, 1024, 2048, or 4096 bits.

See [Section G.1.4.2.1](#) for an example showing the DN syntax.

G.1.4.2.4 Adding a User Certificate to an Oracle Wallet

```
orapki wallet add -wallet wallet_location -user_cert -cert certificate_location
```

This command adds the user certificate at the location specified with the `-cert` parameter to the Oracle wallet at the `wallet_location`. Before you add a user certificate to a wallet, you must add all the trusted certificates that make up the certificate chain. If all trusted certificates are not installed in the wallet before you add the user certificate, then adding the user certificate will fail.

G.1.4.3 Exporting Certificates and Certificate Requests from Oracle Wallets with orapki

This section contains these topics:

- [Exporting a Certificate from an Oracle Wallet](#)
- [Exporting a Certificate Request from an Oracle Wallet](#)

G.1.4.3.1 Exporting a Certificate from an Oracle Wallet

```
orapki wallet export -wallet wallet_location -dn
certificate_dn -cert certificate_filename
```

This command exports a certificate with the subject's distinguished name (`-dn`) from a wallet to a file that is specified by `-cert`.

See [Section G.1.4.2.1](#) for an example showing the DN syntax.

G.1.4.3.2 Exporting a Certificate Request from an Oracle Wallet

```
orapki wallet export -wallet wallet_location -dn
certificate_request_dn -request certificate_request_filename
```

This command exports a certificate request with the subject's distinguished name (`-dn`) from a wallet to a file that is specified by `-request`.

See [Section G.1.4.2.1](#) for an example showing the DN syntax.

G.1.4.4 Creating and Managing Trust Flags

Trust flags allow adequate roles to be assigned to certificates to facilitate operations like certificate chain validation and path building. By default, wallets do not support trust flags.

You can use the `orapki` utility to maintain trust flags in the certificates installed in an Oracle Wallet. You can create and convert wallets to support trust flags, create and maintain appropriate flags in each certificate, and so on.

[Table G-1](#) shows the supported trust flags:

Table G-1 Trust Flags in Oracle Wallet Certificates

Flag	Description	Type
"C"	assigned to trusted CA's certificates, both root and intermediate. Can co-exist with "T" flag.	SERVER_AUTH
"T"	assigned to trusted CA's certificates, both root and intermediate. Can co-exist with "C" flag.	CLIENT_AUTH

Table G-1 (Cont.) Trust Flags in Oracle Wallet Certificates

Flag	Description	Type
"P"	assigned to Peer's user certificate. Cannot co-exist with "C", "T" and "U".	VALID_PEER
"U"	Automatically assigned to the user certificate in the wallet, cannot be added/modified/cleared with orapki tool	USER_CERT
""	Assigned implicitly to certificates that do not have any flag.	NULL

In addition to the flag assignments you can explicitly perform, here are certain assignments automatically made in certificates (when the wallet allows trust flags):

- In a root wallet (with copies of the same certificate in 'user certificates' and 'trusted certificates' section), USER_CERT flag is added to certificate(s) in 'user certificates' section only.
- When a wallet is converted so that it supports trust flags, the following assignments happen:
 - USER_CERT is added to the user certificates as described in the previous bullet
 - NULL is assigned to all the trusted certificates.
- When a new trusted certificate is added to the wallet without specifying any trust flag, NULL is assigned to the certificate.
- When a certificate is deleted from the wallet, all flags associated with the certificate are deleted. If the same certificate is re-installed flags must be added again.
- When a wallet is created with trust flags (using the `-with_trust_flags` option) the wallet is populated with certain default certificates. All these certificates are assigned the `SERVER_AUTH/CLIENT_AUTH` flags.

The following topics explain the trust flag operations you can perform with orapki:

- [Creating a Wallet to Support Trust Flags](#)
- [Converting a Wallet to Support Trust Flags](#)
- [Adding and Updating a Certificate's Trust Flags](#)
- [Adding a Certificate with Trust Flags to Wallet](#)

G.1.4.4.1 Creating a Wallet to Support Trust Flags

```
orapki wallet create -wallet wallet_location
-pwd password -with_trust_flags
```

This command creates an Oracle wallet that supports trust flags; wallets created without the `with_trust_flags` parameter do not support trust flags, but can be converted to do so.

Other options like creating an auto-login wallet can also be specified when creating a wallet to support trust flags.

By default, trusted certificates added to the new wallet are assigned `SERVER_AUTH/CLIENT_AUTH` flags which you can clear explicitly.

G.1.4.4.2 Converting a Wallet to Support Trust Flags

```
orapki wallet enable_trust_flags -wallet wallet_location -pwd password
```

This command converts a wallet to support trust flags. Usage rules are as follows:

Password is not required if it is an auto-login wallet.

After using this command, you cannot convert the wallet back to its original state, that is, to not support trust flags.

All user certificates present in the wallet are assigned the `USER_CERT` flag. All trusted certificate are assigned `NULL` flag. You can change the flags associated with trusted certificates to assign the desired trust flags to these certificates.

Adding Certificates to Empty Wallet

As mentioned earlier, after using this command you cannot convert the wallet back to its original state to not support trust flags.

If you remove all the certificates from the wallet, including the default certificates installed by orapki, the tool can no longer determine whether the wallet supports trust flags. Therefore it is advisable not to remove the default installed certificates from the wallet; if you must remove them, make sure to install a certificate before removing them so at least one certificate remains in the wallet.

If you delete all the certificates from a wallet and later install new certificates, the wallet behaves as follows: If the new certificate is installed with the trust flags option, the wallet will automatically support trust flags. If the new certificate is installed without the trust flags option, the wallet will not support trust flags.

G.1.4.4.3 Adding and Updating a Certificate's Trust Flags

```
orapki wallet assign_trust_flags -wallet wallet_location  
-pwd password -trust_flags ""|"flags"  
-dn "value" [-serial_num "value" -issuer "value"]
```

This command adds, updates, or deletes trust flags for the certificate specified by the dn. Syntax rules are as follows:

- The wallet must support trust flags.
- Password is not required if wallet is an auto-login wallet.
- Specify the flags as defined in [Table G-1](#).
- The Subject DN is the only mandatory certificate attribute parameter, the remaining two parameters being optional. However, you must provide sufficient detail using these parameters to uniquely identify the certificate.
- The matching attribute names are case insensitive, and attribute values are case-sensitive.
- The serial number should be a numeric value.
- Existing flags, if any, assigned to the certificate are over-written.
- Multiple flags can be assigned using ", "(comma); like `-add "SERVER_AUTH, CLIENT_AUTH"`

- USER_CERT flag is not permitted in this command, as this flag is assigned implicitly to the user certificates. For the user certificate the USER_CERT flag shall always be there.
- To remove trust flags, use `-add ""`. The NULL flag is assigned to the certificate.
- If the modify/clear action would result in an invalid certificate chain for any user certificate, the action is not carried out.

For example:

```
orapki wallet assign_trust_flags -wallet /usr/test
-trust_flags "SERVER_AUTH,CLIENT_AUTH"
-dn "cn=jack, ou=people, dc=example, dc=com"
-serial_num "1122" -issuer "sample"
```

G.1.4.4 Adding a Certificate with Trust Flags to Wallet

```
orapki wallet add -wallet wallet_location
-[trusted_cert|user_cert|self_signed]
-cert cert_location -pwd password -trust_flags "flag(s)"
```

This command adds a certificate with specified trust flag(s) to an Oracle wallet. Syntax rules are as follows:

- The wallet must support trust flags.
- Password is not required if wallet is an auto-login wallet.
- `cert_location` is not required if you generate a self signed certificate.
- USER_CERT flag is added implicitly if the certificate is of type `user_cert`. (In a root wallet a self-signed certificate is also present in the 'trusted certificates' section; the USER_CERT flag is *not* assigned to this certificate).
- The flags are specified as defined in [Table G-1](#).
- If trust flags are enabled there is no need for the complete hierarchy of trusted certificates to be present (unlike the case for wallets without trust flags, where the entire chain must be present when adding a user certificate). The certificate chain building stops if a SERVER_AUTH/CLIENT_AUTH flag is assigned to any trusted certificate in the hierarchy.

G.1.4.5 Importing PKCS#12 Files to an Oracle Wallet

```
orapki wallet import_pkcs12
-wallet wallet_location [-pwd wallet_password]
-pkcs12file pkcs12_file_location [-pkcs12pwd pkcs12_file_password]
```

This command imports a PKCS#12 file into an Oracle wallet. The utility prompts you if you do not specify passwords with the command.

G.1.5 Managing Certificate Revocation Lists (CRLs) with orapki Utility

CRLs must be managed with `orapki`. This utility creates a hashed value of the CRL issuer's name to identify the CRLs location in your system. If you do not use `orapki`, your Oracle server cannot locate CRLs to validate PKI digital certificates. The following sections describe CRLs, how you use them, and how to use `orapki` to manage them:

- [Section G.1.5.1, "About Certificate Validation with Certificate Revocation Lists"](#)

- [Section G.1.5.2, "Certificate Revocation List Management"](#)

See Also: "Certificate Revocation List Management" in the *Oracle Advanced Security Administrator's Guide* for details about managing CRLs with orapki:

http://docs.oracle.com/cd/E11882_01/network.112/e10746/asoss1.htm

G.1.5.1 About Certificate Validation with Certificate Revocation Lists

The process of determining whether a given certificate can be used in a given context is referred to as certificate validation. Certificate validation includes determining that:

- A trusted certificate authority (CA) has digitally signed the certificate.
- The certificate's digital signature corresponds to the independently-calculated hash value of the certificate itself and the certificate signer's (CA's) public key.
- The certificate has not expired.
- The certificate has not been revoked.

The SSL network layer automatically performs the first three validation checks, but you must configure certificate revocation list (CRL) checking to ensure that certificates have not been revoked. CRLs are signed data structures that contain a list of revoked certificates. They are usually issued and signed by the same entity who issued the original certificate.

G.1.5.1.1 What CRLs Should You Use? You should have CRLs for all of the trust points that you honor. The trust points are the trusted certificates from a third-party identity that is qualified with a level of trust. Typically, the certificate authorities you trust are called trust points.

G.1.5.1.2 How CRL Checking Works Certificate revocation status is checked against CRLs which are located in file system directories, or downloaded from the location specified in the CRL Distribution Point (CRL DP) extension on the certificate. If you store your CRLs on the local file system or in the directory, then you must update them regularly. If you use CRL DPs then CRLs are downloaded when the corresponding certificates are first used.

The server searches for CRLs in the following locations in the order listed. When the system finds a CRL that matches the certificate CA's DN, it stops searching.

1. Local file system

The locations and management of CRL files is component-dependent. For Oracle WebLogic Server, see "Configuring the CRL Local Cache" in *Administering Security for Oracle WebLogic Server*. For Oracle HTTP Server, see Doc ID 1665286.1, "How to Configure CRL Checking in Oracle HTTP Server in FMW 12c" in the Oracle Technology Network Knowledge Base.

2. CRL DP

If the CA specifies a location in the CRL DP X.509, version 3, certificate extension when the certificate is issued, then the appropriate CRL that contains revocation information for that certificate is downloaded. Currently, Oracle Advanced Security supports downloading CRLs over HTTP and LDAP.

Notes:

- For performance reasons, only user certificates are checked.
 - Oracle recommends that you store CRLs in the directory rather than the local file system.
-
-

G.1.5.2 Certificate Revocation List Management

Procedures for CRL management depend on the component in question. For Oracle WebLogic Server, see "Configuring the CRL Local Cache" in *Administering Security for Oracle WebLogic Server*. For Oracle HTTP Server, see Doc ID 1665286.1, "How to Configure CRL Checking in Oracle HTTP Server in FMW 12c" in the Oracle Technology Network Knowledge Base.

Before you can enable certificate revocation status checking, you must ensure that the CRLs you receive from the CAs you use are in a form (renamed with a hash value) or in a location (uploaded to the directory) in which your system can use them. Oracle Advanced Security provides a command-line utility, `orapki`, that you can use to perform the following task:

- [Renaming CRLs with a Hash Value for Certificate Validation](#)

Note: CRLs must be updated at regular intervals (before they expire) for successful validation. You can automate this task by using `orapki` commands in a script.

See Also: Command-Line Tools Overview in the *Oracle Fusion Middleware Reference for Oracle Identity Management* for information about LDAP command-line tools and their syntax.

G.1.5.2.1 Renaming CRLs with a Hash Value for Certificate Validation When the system validates a certificate, it must locate the CRL issued by the CA who created the certificate. The system locates the appropriate CRL by matching the issuer name in the certificate with the issuer name in the CRL.

When you specify a CRL storage location for the **Certificate Revocation Lists Path** field in Oracle Net Manager (sets the `SSL_CRL_PATH` parameter in the `sqlnet.ora` file), use the `orapki` utility to rename CRLs with a hash value that represents the issuer's name. Creating the hash value enables the server to load the CRLs.

On UNIX systems, `orapki` creates a symbolic link to the CRL. On Windows systems, it creates a copy of the CRL file. In either case, the symbolic link or the copy created by `orapki` are named with a hash value of the issuer's name. Then when the system validates a certificate, the same hash function is used to calculate the link (or copy) name so the appropriate CRL can be loaded.

Depending on your operating system, enter one of the following commands to rename CRLs stored in the file system.

To rename CRLs stored in UNIX file systems:

```
orapki crl hash -crl crl_filename [-wallet wallet_location]
-symlink crl_directory [-summary]
```

To rename CRLs stored in Windows file systems:

```
orapki crl hash -crl crl_filename  
[-wallet wallet_location] -copy crl_directory [-summary]
```

In the preceding commands, *crl_filename* is the name of the CRL file, *wallet_location* is the location of a wallet that contains the certificate of the CA that issued the CRL, and *crl_directory* is the directory in which the CRL is located.

Using `-wallet` and `-summary` are optional. Specifying `-wallet` causes the tool to verify the validity of the CRL against the CA's certificate prior to renaming the CRL. Specifying the `-summary` option causes the tool to display the CRL issuer's name.

G.1.6 orapki Utility Commands Summary

This section lists and describes the following `orapki` commands:

- `orapki cert create`
- `orapki cert display`
- `orapki crl create`
- `orapki crl hash`
- `orapki crl revoke`
- `orapki crl status`
- `orapki crl verify`
- `orapki wallet add`
- `orapki wallet change_pwd`
- `orapki wallet create`
- `orapki wallet enable_trust_flags`
- `orapki wallet assign_trust_flags`
- `orapki wallet display`
- `orapki wallet export`
- `orapki wallet export_trust_chain`
- `orapki wallet import_pkcs12`

G.1.6.1 orapki cert create

The following sections describe this command.

G.1.6.1.1 Purpose Use this command to create a signed certificate for testing purposes.

G.1.6.1.2 Syntax `orapki cert create [-wallet wallet_location]
-request certificate_request_location
-cert certificate_location -validity number_of_days [-summary]`

- The `-wallet` parameter specifies the wallet containing the user certificate and private key that will be used to sign the certificate request.
- The `-request` parameter (mandatory) specifies the location of the certificate request for the certificate you are creating.
- The `-cert` parameter (mandatory) specifies the directory location in which the tool places the new signed certificate.

- The `-validity` parameter (mandatory) specifies the number of days, starting from the current date, that this certificate will be valid.

G.1.6.2 orapki cert display

The following sections describe this command.

G.1.6.2.1 Purpose Use this command to display details of a specific certificate.

G.1.6.2.2 Syntax `orapki cert display -cert certificate_location [-summary|-complete]`

- The `-cert` parameter specifies the location of the certificate you want to display.
- You can use either the `-summary` or the `-complete` parameter to display the following information:
 - `-summary` displays the certificate and its expiration date
 - `-complete` displays additional certificate information, including the serial number and public key

G.1.6.3 orapki crl create

The following sections describe this command.

G.1.6.3.1 Purpose Use this command to create a CRL.

G.1.6.3.2 Syntax `orapki crl create [-crl [url/filename]] [-wallet [cawallet]] [-nextupdate [days]] [-pwd pwd]`

- `-crl` is the location where the CRL will be created (for example `./nzcrl.txt`)
- `-wallet` is the `cawallet`, which contains self-signed certificate and corresponding private key
- `-nextupdate` is the number of days until the next update
- `-pwd` is the password of `cawallet`

G.1.6.4 orapki crl hash

The following sections describe this command.

G.1.6.4.1 Purpose Use this command to generate a hash value of the certificate revocation list (CRL) issuer to identify the location of the CRL in your file system for certificate validation.

G.1.6.4.2 Syntax `orapki crl hash -crl crl_filename/URL [-wallet wallet_location] [-symlink|-copy] crl_directory [-summary]`

- The `-crl` parameter specifies the filename that contains the CRL or the URL in which it can be found.
- The `-wallet` parameter (optional) specifies the location of the wallet that contains the certificate of the certificate authority (CA) who issued the CRL. Using it causes the tool to verify the validity of the CRL against the CA's certificate prior to uploading it to the directory.

- Depending on your operating system, use either the `-symlink` or the `-copy` parameter:
 - On UNIX: Use `-symlink` to create a symbolic link to the CRL at the `crl_directory` location
 - On Windows: Use `-copy` to create a copy of the CRL at the `crl_directory` location
- The `-summary` parameter (optional) causes the tool to display the CRL issuer's name.

G.1.6.5 orapki crl revoke

The following sections describe this command.

G.1.6.5.1 Purpose Use this command to revoke a certificate.

G.1.6.5.2 Syntax `orapki crl revoke [-crl [url|filename]]`
`[-wallet [cawallet]]`
`[-cert [revokecert]]`
`[-pwd pwd]`

where:

- `-crl` specifies the CRL as either a URL or a filename
- `-wallet` is the `cawallet`, which contains self-signed certificate and corresponding private key
- `-cert`: certificate to be revoked
- `-pwd` is the password of `cawallet`.

G.1.6.6 orapki crl status

The following sections describe this command.

G.1.6.6.1 Purpose Use this command to check if a certificate is revoked in a CRL.

G.1.6.6.2 Syntax `orapki crl status [-crl [url|filename]]`
`[-cert [cert]]`

- `-crl` specifies the CRL as either a URL or a filename
- `-cert` is the CA's certificate

G.1.6.7 orapki crl verify

The following sections describe this command.

G.1.6.7.1 Purpose Use this command to verify a CRL signature.

G.1.6.7.2 Syntax `orapki crl verify [-crl [url|filename]]`
`[-cert [cacert]]`

where:

- `-crl` specifies the CRL as either a URL or a filename
- `-cert` specifies the certificate to be checked

G.1.6.8 orapki wallet add

The following sections describe this command.

G.1.6.8.1 Purpose Use this command to add certificate requests and certificates to an Oracle wallet.

G.1.6.8.2 Syntax

See Also: See [Section G.1.4.2.1](#) for an example showing the DN syntax.

To add certificate requests:

```
orapki wallet add -wallet wallet_location -dn user_dn -keysize 512|1024|2048
```

- The `-wallet` parameter specifies the location of the wallet to which you want to add a certificate request.
- The `-dn` parameter specifies the distinguished name of the certificate owner.
- The `-keysize` parameter specifies the key size for the certificate.
- To sign the request, export it with the export option. See [Section G.1.6.14, "orapki wallet export"](#).

To add trusted certificates:

```
orapki wallet add -wallet wallet_location -trusted_cert -cert certificate_location
```

- The `-trusted_cert` parameter causes the tool to add the trusted certificate, at the location specified with `-cert`, to the wallet.

To add root certificates:

```
orapki wallet add -wallet wallet_location -dn
certificate_dn -keysize 512|1024|2048 -self_signed
-valid_from [mm/dd/yyyy] -valid_until [mm/dd/yyyy]
-validity number_of_days
```

- The `-self_signed` parameter causes the tool to create a root certificate.
- The `-validity` parameter can be used to specify the number of days, starting from the current date, that this root certificate will be valid.
- The `-valid_from` and `valid_until` parameters can be used to specify an exact date range for which this root certificate will be valid. You may specify validity in this way instead of `-validity number_of_days`.

To add user certificates:

```
orapki wallet add -wallet wallet_location -user_cert -cert certificate_location
```

- The `-user_cert` parameter causes the tool to add the user certificate at the location specified with the `-cert` parameter to the wallet. Before you add a user certificate to a wallet, you must add all the trusted certificates that make up the certificate chain. If all trusted certificates are not installed in the wallet before you add the user certificate, then adding the user certificate will fail.

To add a subject key identifier extension to a certificate request:

```
orapki wallet add -wallet wallet_location -dn user_dn -keysize 512|1024|2048
-addext_ski
```

To add a Version 3 self-signed certificate to a wallet:

```
orapki wallet add -wallet wallet_location -dn certificate_dn -keysize  
512|1024|2048 -self_signed -validity number_of_days -addext_ski
```

To add trust flags while adding a certificate to a wallet:

```
orapki wallet add -wallet wallet_location  
-[trusted_cert|user_cert|self_signed]  
-cert cert_location -pwd password -trust_flags "flag(s)"
```

- The `-trust_flags` parameter causes the specified flags to be added to the certificate. See [Section G.1.4.4.4](#) for usage details.

See [Section G.1.4.2.1](#) for an example showing the DN syntax.

G.1.6.9 orapki wallet change_pwd

The following sections describe this command.

G.1.6.9.1 Purpose Use this command to change the password for an Oracle wallet.

G.1.6.9.2 Syntax `orapki wallet change_pwd [-wallet wallet_location] [-oldpwd oldpassword] [-newpwd newpassword]`

- The `-wallet` parameter specifies the location of the wallet whose password you want to change.
- The `-oldpwd` parameter specifies the existing wallet password.
- The `-newpwd` parameter specifies the new wallet password.

G.1.6.10 orapki wallet create

The following sections describe this command.

G.1.6.10.1 Purpose Use this command to create an Oracle wallet, to set auto-login on for an Oracle wallet, and to enable trust flags for certificates.

G.1.6.10.2 Syntax `orapki wallet create -wallet wallet_location
[-with_trust_flags] [-auto_login]`

- The `-wallet` parameter specifies a location for the new wallet or the location of the wallet for which you want to turn on auto-login.
- The `-auto_login` parameter creates an auto-login wallet, or it turns on automatic login for the wallet specified with the `-wallet` option.
- The `-with_trust_flags` parameter enables the wallet to support trust flags.

G.1.6.11 orapki wallet enable_trust_flags

The following sections describe this command.

G.1.6.11.1 Purpose Use this command to convert a wallet to support trust flags.

G.1.6.11.2 Syntax `orapki wallet enable_trust_flags -wallet wallet_location -pwd
password`

G.1.6.12 orapki wallet assign_trust_flags

The following sections describe this command.

G.1.6.12.1 Purpose Use this command to assign trust flags to a certificate in a wallet.

G.1.6.12.2 Syntax `orapki wallet assign_trust_flags -wallet wallet_location
-pwd password -trust_flags "|"flags"
-dn "value" [-serial_num "value" -issuer "value"]`

- The `-dn` parameter is required.
- The `-serial_num` and `-issuer` parameters may be required to uniquely match a single certificate in the wallet.

For additional usage details, see [Section G.1.4.4.3](#).

See [Section G.1.4.2.1](#) for an example showing the DN syntax.

G.1.6.13 orapki wallet display

The following sections describe this command.

G.1.6.13.1 Purpose Use this command to view the certificate requests, user certificates, and trusted certificates in an Oracle wallet.

G.1.6.13.2 Syntax `orapki wallet display -wallet wallet_location`

- The `-wallet` parameter specifies a location for the wallet you want to open if it is not located in the current working directory.

G.1.6.14 orapki wallet export

The following sections describe this command.

See Also: [Section G.1.4.2.1](#) for examples of specifying the `dn` parameter.

G.1.6.14.1 Purpose

Use this command to export certificate requests and certificates from an Oracle wallet.

G.1.6.14.2 Syntax

```
orapki wallet export -wallet wallet_location  
-dn certificate_dn -cert certificate_filename
```

- The `-wallet` parameter specifies the directory where the wallet, from which you want to export the certificate, is located.
- The `-dn` parameter specifies the distinguished name of the certificate.
- The `-cert` parameter specifies the path and filename of the file that contains the exported certificate.

To export a certificate request from an Oracle wallet:

```
orapki wallet export -wallet wallet_location  
-dn certificate_request_dn -request certificate_request_filename
```

- The `-request` parameter specifies the path and filename of the file that contains the exported certificate request.

G.1.6.15 orapki wallet export_trust_chain

The following sections describe this command.

G.1.6.15.1 Purpose

Use this command to export a chain of trust (certificate chain) for a user.

G.1.6.15.2 Syntax

```
orapki wallet export_trust_chain [-wallet [wallet]]
[-certchain [filename]]
[-dn [user_cert_dn] ]
[-pwd pwd]
```

- The `-wallet` parameter specifies the location of the wallet from which you want to export the certificate chain.
- The `-certchain` parameter specifies the name of the file to contain the exported certificate chain.
- The `-dn` parameter specifies the distinguished name of the entry to be exported.
- The `-pwd` specifies the wallet password.

See [Section G.1.4.2.1](#) for an example of how to specify the `-dn` parameter.

G.1.6.16 orapki wallet import_pkcs12

The following sections describe this command.

G.1.6.16.1 Purpose

Use this command to import a PKCS#12 file into an Oracle wallet.

G.1.6.16.2 Syntax

```
orapki wallet import_pkcs12
-wallet wallet_location [-pwd wallet_password]
-pkcs12file pkcs12_file_location [-pkcs12pwd pkcs12_file_password]
```

- The `wallet` parameter specifies the relative or absolute path of Oracle Wallet into which PKCS#12 file is to be imported. Required.
- The `pwd` parameter specifies the password of Oracle Wallet into which PKCS#12 file is to be imported. Optional, prompts as needed.
- The `pkcs12file` parameter specifies the relative or absolute path of PKCS#12 file to be imported into Oracle Wallet. Required.
- The `pkcs12pwd` parameter specifies the password of PKCS#12 file that is to be imported into Oracle Wallet. Optional, prompts as needed.

For example:

```
orapki wallet import_pkcs12 -wallet /scratch/user/oracleWalletFolder/ewallet.p12
-pwd walletPassword -pkcs12file /scratch/userId/pkcs12fileFolder/certandkey.p12
-pkcs12pwd pkcs12filePassword
```

Troubleshooting Oracle Fusion Middleware

This appendix provides information on how to troubleshoot problems that you might encounter when using Oracle Fusion Middleware. It contains the following sections:

- [Section H.1, "Diagnosing Oracle Fusion Middleware Problems"](#)
- [Section H.2, "Common Problems and Solutions"](#)
- [Section H.3, "Troubleshooting SSL"](#)
- [Section H.4, "Troubleshooting FIPS Configuration"](#)
- [Section H.5, "Need More Help?"](#)

H.1 Diagnosing Oracle Fusion Middleware Problems

Oracle Fusion Middleware components generate log files containing messages that record all types of events, including startup and shutdown information, errors, warning messages, access information on HTTP requests, and additional information. The log files can be used to identify and diagnose problems. See [Chapter 12, "Managing Log Files and Diagnostic Data"](#) for more information about using and reading log files.

Oracle Fusion Middleware includes a Diagnostic Framework which aids in detecting, diagnosing, and resolving problems. The problems that are targeted in particular are critical errors such as those caused by code bugs, metadata corruption, and customer data corruption, deadlocked threads, and inconsistent state.

When a critical error occurs, it is assigned an incident number, and diagnostic data for the error (such as log files) are immediately captured and tagged with this number. The data is then stored in the Automatic Diagnostic Repository (ADR), where it can later be retrieved by incident number and analyzed. See [Chapter 13, "Diagnosing Problems"](#) for more information about the Diagnostic Framework.

H.2 Common Problems and Solutions

This section describes common problems and solutions. It contains the following topics:

- [Running out of Data Source Connections](#)
- [Using a Different Version of Spring](#)
- [ClassNotFoundExceptions When Starting Managed Servers](#)

H.2.1 Running out of Data Source Connections

If the database performance has slowed or you receive the following message in the Oracle WebLogic Server log files, you may have leaks in the data source connections:

```
No resources currently available in pool datasource name
```

Any product functionality that depend on the datasource will not function as it can't connect database to get required data.

If you receive this message, monitor the connection usage from the Administration Console data source monitoring page:

1. From Domain Structure, expand **Services**, then **Data Sources**.
2. Click the data source that you want to monitor.
3. Select the Monitoring tab, then the Statistics tab.
4. If the table does not display **Active Connection Current Count**, click **Customize this table**.
5. In Column Display, select **Active Connection Current Count** and move it from the Available to the Chosen box. Click **Apply**.
6. In the table, note the number in the **Active Connection Current Count** column.

If the active current count for a data source keeps increasing and does not go down, this data source is leaking connections. Contact Oracle Support.

H.2.2 Using a Different Version of Spring

When you configure a Managed Server with JRF, Spring 2.0.6 is installed and is placed in the Oracle WebLogic Server system classpath. If a custom application running in a JRF environment requires a different version of Spring, you must use the Filtering ClassLoader mechanism to specify the version of Spring.

Oracle WebLogic Server provides the FilteringClassLoader mechanism so that you can configure deployment descriptors to explicitly specify that certain packages should always be loaded from the application, rather than being loaded by the system classloader. This allows you to use alternate versions of applications such as Spring or Ant.

For more information about using the FilteringClassLoader mechanism, see "Using a Filtering ClassLoader" in *Developing Applications for Oracle WebLogic Server*.

H.2.3 ClassNotFoundException Errors When Starting Managed Servers

If a Managed Server is started by Node Manager (as is the case when the servers are started by the Oracle WebLogic Server Administration Console or Fusion Middleware Control), you may receive a ClassNotFoundException error if Node Manager has not been configured to use the start scripts when starting Managed Servers. See [Section 2.7.1](#) for information about resolving this problem.

H.3 Troubleshooting SSL

This section describes common problems and solutions when working with SSL configuration. It contains the following topics:

- [Components May Enable All Supported Ciphers](#)
- [SSL Certificate Chain Required on Certain Browsers](#)

- [keyUsage Extension Required for Certificates in JDK7](#)

H.3.1 Components May Enable All Supported Ciphers

You should be aware that when no cipher is explicitly configured, some 12c (12.1.3) components enable all supported SSL ciphers including DH_Anon (Diffie-Hellman Anonymous) ciphers.

At this time, Oracle HTTP Server is the only component known to set ciphers like this.

Configure the components with the desired cipher(s) if DH_Anon is not wanted.

H.3.2 SSL Certificate Chain Required on Certain Browsers

When you configure SSL for Oracle HTTP Server, you may need to import the entire certificate chain (rootCA, Intermediate CAs and so on).

Certain browsers, for example Internet Explorer, require that the entire certificate chain be imported to the browsers for SSL handshake to work. If your certificate was issued by an intermediate CA, you will need to ensure that the complete chain of certificates is available on the browser or the handshake will fail. If an intermediate certificate in the chain expires, it must be renewed along with all the certificates in the chain ((such as the OHS server certificate).

H.3.3 keyUsage Extension Required for Certificates in JDK7

In JDK6, a self-signed certificate can contain the `keyUsage` extension without enabling the `keyCertSign` bit. This is rejected in JDK7.

Under JDK7, if using self-signed CA certificates, ensure that the `keyCertSign` bit of the `keyUsage` extension is set. Otherwise connections fail with an exception such as:

```
weblogic.common.resourcepool.ResourceDeadException:
0:weblogic.common.ResourceException: Could not create pool connection. The
DBMS driver exception was: IO Error:
sun.security.validator.ValidatorException: PKIX path validation failed:
java.security.cert.CertPathValidatorException: Path does not chain with any
of the trust anchors
```

The key usage extension defines the purpose (for example enciphering, signature, certificate signing) of the key contained in the certificate.

Conforming CAs must include this extension in certificates that contain public keys that are used to validate digital signatures on other public key certificates or CRLs.

The `keyCertSign` bit is asserted when the subject public key is used for verifying signatures on public key certificates. When generating self-signed CA certificates in JDK7, therefore, you must ensure that the `keyCertSign` bit of `keyUsage` is on.

You can achieve this, for example, by:

1. Creating a self-signed JKS keystore with option `ku:c=keyCertSign`, and
2. migrating the certificate from the keystore to the root wallet which will be used by the SSL DB connection

```
orapki wallet jks_to_pkcs12 -wallet ./ -pwd password -keystore ./ewallet.jks
-jkspwd password
```

H.4 Troubleshooting FIPS Configuration

For details about this topic, see [Section 8.5](#).

H.5 Need More Help?

You can find more solutions on My Oracle Support, <http://support.oracle.com>. If you do not find a solution for your problem, log a service request.

You can also use the Remote Diagnostic Agent, as described in [Section H.5.1](#).

H.5.1 Using Remote Diagnostic Agent

Remote Diagnostic Agent (RDA) is a command-line diagnostic tool that provides a comprehensive picture of your environment. Additionally, RDA can provide recommendations on various topics, for example configuration and security. This aids you and Oracle Support in resolving issues.

RDA is designed to be as unobtrusive as possible; it does not modify systems in any way. A security filter is provided if required.

For more information about RDA, see the readme file, which is located at:

```
(UNIX) ORACLE_HOME/oracle_common/rda/README_Unix.txt  
(Windows) ORACLE_HOME\oracle_common\rda\README_Windows.txt
```