

Oracle® Enterprise Manager
Lifecycle Management Administrator's Guide
12c Release 2 (12.1.0.2)
E27046-08

September 2012

Oracle Enterprise Manager Lifecycle Management Administrator's Guide, 12c Release 2 (12.1.0.2)

E27046-08

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

Primary Author: Aravind Jayaraaman

Contributing Author: Genevieve D'Souza, Aparna Kamath, Pushpa Raghavachar, Namrata Bhakthavatsalam, Jacqueline Gosselin, Jim Garrison, Leo Cloutier

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

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

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

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

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

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

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

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

Contents

Preface	xxvii
Audience	xxvii
Documentation Accessibility	xxvii
Related Documents	xxvii
Conventions	xxviii

Part I Overview and Setup Details

1 Introduction to Lifecycle Management

1.1 Overview of the New Lifecycle Management Solutions	1-1
1.2 Information Map	1-4

2 Setting Up Your Infrastructure

2.1 Getting Started	2-1
2.2 Setting Up Oracle Software Library	2-2
2.3 Setting Up Credentials	2-4
2.3.1 Setting Up Named Credentials	2-6
2.3.2 Setting Up Privileged Credentials	2-8
2.3.3 Configuring Privilege Delegation Settings	2-9
2.3.3.1 Using Privilege Delegation	2-10
2.3.3.2 Setting up Privilege Delegation	2-10
2.3.3.3 Creating Privilege Delegation Templates	2-12
2.3.3.4 Testing Privilege Delegation Settings	2-13
2.3.4 Saving Preferred Credentials	2-14
2.3.4.1 Saving Preferred Credentials for Hosts and Oracle Homes	2-14
2.3.4.2 Saving Preferred Credentials to Access My Oracle Support	2-16
2.4 Creating Enterprise Manager User Accounts	2-16
2.4.1 Overview of User Accounts	2-17
2.4.2 Creating Designer User Account	2-18
2.4.3 Creating Operator User Account	2-19
2.5 Setting Up My Oracle Support	2-19
2.6 (Additional) Configuring Self-Update	2-19
2.7 (Additional) Setting Up E-mail Notifications	2-20

Part II Discovery

3 Discovering Software Deployments

3.1	Discovering Hosts and Targets Automatically.....	3-1
3.2	Discovering Hosts and Targets Manually	3-1

Part III Database Provisioning

4 Overview of Database Provisioning

4.1	Overview of Database Provisioning Feature	4-1
4.2	Supported Targets and Deployment Procedures for Database Provisioning.....	4-3
4.3	Setting Up Database Provisioning.....	4-5
4.3.1	Meeting Basic Infrastructure and Host Requirements	4-6
4.3.2	Understanding Administrator Privileges for Provisioning Database	4-6
4.3.3	Prerequisites for Designers.....	4-7
4.3.4	Prerequisites for Operators	4-8
4.3.5	Creating Provisioning Profiles.....	4-9
4.3.6	Creating Installation Media.....	4-10
4.3.7	Creating Database Templates	4-12
4.3.8	Uploading Database Templates to Software Library	4-13
4.3.9	Creating Database Provisioning Entities.....	4-14
4.3.9.1	Creating an Oracle Database Clone from a Reference Home	4-14
4.3.9.2	Creating an Oracle Database Clone from an External Storage	4-15
4.3.9.3	Creating an Oracle Clusterware Clone from a Reference Home.....	4-16
4.3.9.4	Creating an Oracle Clusterware Clone from an External Storage.....	4-17
4.3.10	Downloading Cluster Verification Utility.....	4-18

5 Provisioning Oracle Databases

5.1	Getting Started.....	5-1
5.2	Oracle Database Topology.....	5-2
5.3	Provisioning and Creating Oracle Databases	5-3
5.3.1	Prerequisites	5-3
5.3.2	Provisioning Procedure	5-3
5.4	Provisioning Oracle Databases with Oracle Automatic Storage Management	5-8
5.4.1	Prerequisites	5-8
5.4.2	Provisioning Procedure	5-8
5.5	Provisioning Oracle Database Software Only	5-13
5.5.1	Prerequisites	5-13
5.5.2	Provisioning Procedure	5-13

6 Provisioning Oracle Grid Infrastructure for Oracle Databases

6.1	Getting Started.....	6-1
6.2	Provisioning Oracle Grid Infrastructure and Oracle Databases with Oracle Automatic Storage Management 6-2	
6.2.1	Prerequisites	6-2
6.2.2	Provisioning Procedure	6-2
6.3	Provisioning Oracle Grid Infrastructure and Oracle Database Software Only	6-7
6.3.1	Prerequisites	6-8

6.3.2	Provisioning Procedure	6-8
-------	------------------------------	-----

7 Provisioning Oracle Grid Infrastructure for Oracle Real Application Clusters Databases

7.1	Getting Started.....	7-1
7.2	Oracle Real Application Clusters Database Topology	7-2
7.3	Provisioning Grid Infrastructure with Oracle Real Application Clusters Database and Configuring Database with Oracle Automatic Storage Management 7-3	
7.3.1	Prerequisites	7-3
7.3.2	Procedure	7-4
7.3.2.1	Requirements for Grid Infrastructure Software Location Path	7-11
7.4	Provisioning Oracle Real Application Clusters Database with File System on an Existing Cluster 7-11	
7.4.1	Prerequisites	7-11
7.4.2	Procedure	7-11
7.5	Provisioning Oracle Real Application Clusters Database with File System on a New Cluster 7-16	
7.5.1	Prerequisites	7-16
7.5.2	Procedure	7-16

8 Provisioning Oracle Real Application Clusters One (Oracle RAC One) Node Databases

8.1	Getting Started.....	8-1
8.2	Deployment Procedures	8-2
8.3	Provisioning Oracle Real Application Clusters One Node Databases.....	8-2
8.3.1	Prerequisites	8-2
8.3.2	Procedure	8-4

9 Provisioning Oracle Real Application Clusters for 10g and 11g

9.1	Getting Started.....	9-1
9.2	Core Components Deployed	9-2
9.3	Cloning a Running Oracle Real Application Clusters	9-2
9.3.1	Prerequisites	9-2
9.3.2	Cloning Procedure.....	9-4
9.4	Provisioning Oracle Real Application Clusters Using Gold Image	9-9
9.4.1	Prerequisites	9-9
9.4.2	Provisioning Procedure	9-10
9.5	Provisioning Oracle Real Application Clusters Using Archived Software Binaries.....	9-15
9.5.1	Prerequisites	9-15
9.5.2	Provisioning Procedure	9-16
9.5.2.1	Sample Cluster Configuration File.....	9-23

10 Extending Oracle Real Application Clusters

10.1	Getting Started.....	10-1
10.2	Extending Oracle Real Application Clusters	10-1
10.2.1	Prerequisites	10-2

10.2.2	Procedure	10-2
--------	-----------------	------

11 Deleting or Scaling Down Oracle Real Application Clusters

11.1	Getting Started.....	11-1
11.2	Core Components Deleted	11-2
11.3	Deleting the Entire Oracle RAC	11-2
11.3.1	Prerequisites	11-2
11.3.2	Procedure	11-3
11.4	Scaling Down Oracle RAC by Deleting Some of Its Nodes.....	11-5
11.4.1	Prerequisites	11-5
11.4.2	Procedure	11-6

12 Provisioning Oracle Database Replay Client

12.1	Getting Started.....	12-1
12.2	Cloning a Running Oracle Database Replay Client.....	12-2
12.2.1	Prerequisites	12-2
12.2.2	Cloning Procedure.....	12-3
12.3	Provisioning Oracle Database Replay Client Using Gold Image	12-5
12.3.1	Prerequisites	12-5
12.3.2	Provisioning Procedure	12-6
12.4	Provisioning Oracle Database Replay Client Using Installation Binaries	12-8
12.4.1	Prerequisites	12-8
12.4.2	Provisioning Procedure	12-9

13 Creating Databases

13.1	Getting Started.....	13-1
13.2	Creating Oracle Database	13-2
13.2.1	Prerequisites for Creating Oracle Database	13-2
13.2.2	Procedure for Creating Oracle Database.....	13-2
13.3	Creating Oracle Real Application Clusters Database	13-5
13.3.1	Prerequisites for Creating Oracle Real Application Clusters Database.....	13-5
13.3.2	Procedure for Creating Oracle Real Application Clusters Database	13-6
13.4	Creating Oracle Real Application Clusters One Node Database.....	13-8
13.4.1	Prerequisites for Creating Oracle RAC One Node Database	13-8
13.4.2	Procedure for Creating Oracle Real Application Clusters One Node Database	13-9

Part IV Database Upgrade

14 Upgrading Databases

14.1	Getting Started.....	14-1
14.2	Supported Releases.....	14-3
14.3	Deployment Procedure	14-3
14.4	Upgrading Multiple Oracle Database Instances at a Time (Mass Upgrade).....	14-4
14.4.1	Prerequisites	14-4
14.4.2	Upgrade Procedure	14-4
14.5	Upgrading One Oracle Database or One Oracle RAC Database Instance at a Time	14-8

14.5.1	Prerequisites	14-9
14.5.2	Upgrade Procedure	14-9

Part V Middleware Provisioning

15 Provisioning WebLogic Domains and Middleware Homes

15.1	Getting Started.....	15-1
15.2	Middleware Provisioning Deployment Procedures	15-3
15.3	Supported Releases.....	15-4
15.4	Prerequisites for Designers and Operators	15-4
15.4.1	Prerequisites for Designers.....	15-4
15.4.2	Prerequisites for Operators	15-5
15.4.3	Additional Prerequisites on Windows	15-6
15.5	Creating Software Library Components	15-6
15.5.1	Creating a WebLogic Domain Provisioning Profile	15-6
15.5.2	Creating an Oracle Middleware Home Gold Image	15-8
15.6	Cloning from an Existing Installation.....	15-10
15.6.1	Cloning a WebLogic Domain from an Existing Installation	15-10
15.6.1.1	Prerequisites	15-11
15.6.1.2	Deployment Procedure.....	15-11
15.6.2	Cloning a Middleware Home from an Existing Installation	15-18
15.6.2.1	Prerequisites	15-18
15.6.2.2	Deployment Procedure.....	15-19
15.7	Cloning from a Profile or a Middleware Home Gold Image.....	15-20
15.7.1	Cloning from a WebLogic Domain Provisioning Profile.....	15-21
15.7.1.1	Prerequisites	15-21
15.7.1.2	Deployment Procedure.....	15-22
15.7.2	Cloning from an Oracle Middleware Home Gold Image.....	15-23
15.7.2.1	Prerequisites	15-23
15.7.2.2	Deployment Procedure.....	15-23
15.8	Post Deployment Configuration.....	15-26
15.9	Customizing the Deployment Procedure.....	15-26
15.10	Creating an Oracle Virtual Server Component	15-29

16 Scaling Up / Scaling Out WebLogic Domains

16.1	About Scaling Up / Scaling Out WebLogic Domains.....	16-1
16.2	Prerequisites for Designers and Operators	16-1
16.2.1	Prerequisites for Designers.....	16-2
16.2.2	Prerequisites for Operators	16-2
16.2.3	Additional Prerequisites on Windows	16-3
16.3	Prerequisites for the Deployment Procedure.....	16-3
16.4	Running the Scale Up / Scale Out Middleware Deployment Procedure.....	16-4
16.5	Middleware Provisioning and Scale Up / Scale Out Best Practices.....	16-6

17 Deploying / Redeploying / Undeploying Java EE Applications

17.1	Deploying, Undeploying, or Redeploying Java EE Applications.....	17-1
------	--	------

17.2	Getting Started.....	17-1
17.3	Prerequisites	17-2
17.4	Creating a Java EE Application Component.....	17-3
17.5	Java EE Applications Deployment Procedure	17-4
17.5.1	Deploying a Java EE Application	17-4
17.5.2	Redeploying a Java EE Application	17-8
17.5.3	Undeploying a Java EE Application	17-10

18 Provisioning Coherence Nodes and Clusters

18.1	Getting Started.....	18-1
18.2	Supported Releases.....	18-2
18.3	Deploying Coherence Nodes and Clusters	18-2
18.3.1	Prerequisites	18-2
18.3.2	Creating a Coherence Component	18-3
18.3.3	Deployment Procedure	18-4
18.3.3.1	Adding a Coherence Node.....	18-7
18.3.3.2	Sample Scripts	18-10
18.3.3.2.1	default-start-script.pl	18-10
18.3.3.2.2	generate-wka-override.pl.....	18-14
18.4	Troubleshooting	18-16

19 Provisioning SOA Artifacts and Composites

19.1	Understanding SOA Artifacts Provisioning	19-1
19.2	Getting Started.....	19-2
19.3	Deployment Procedures, Supported Releases, and Core Components Deployed	19-3
19.4	Provisioning SOA Artifacts	19-4
19.4.1	Provisioning from a Reference Installation.....	19-4
19.4.1.1	Prerequisites	19-4
19.4.1.2	Provisioning Procedure	19-4
19.4.2	Provisioning SOA Artifacts from Gold Image	19-6
19.4.2.1	Prerequisites	19-6
19.4.2.2	Provisioning Procedure	19-7
19.5	Deploying SOA Composites	19-8
19.5.1	Prerequisites	19-9
19.5.2	Provisioning Procedure	19-9

20 Provisioning Oracle Service Bus Resources

20.1	Getting Started.....	20-1
20.2	Deployment Procedure	20-2
20.3	Supported Releases.....	20-2
20.4	Provisioning Oracle Service Bus Resources from Oracle Service Bus Domain	20-3
20.4.1	Prerequisites	20-3
20.4.2	Provisioning Procedure	20-3
20.4.2.1	Understanding Export Modes	20-6
20.5	Provisioning Oracle Service Bus Resources from Oracle Software Library.....	20-7
20.5.1	Prerequisites	20-7

20.5.2	Provisioning Procedure	20-8
--------	------------------------------	------

21 Provisioning Oracle BPEL Processes

21.1	Getting Started.....	21-1
21.2	Deployment Procedure	21-2
21.3	Supported Releases.....	21-2
21.4	Provisioning Oracle BPEL Processes.....	21-2
21.4.1	Prerequisites	21-2
21.4.2	Provisioning Procedure	21-3

22 Provisioning Oracle Application Server

22.1	Getting Started.....	22-1
22.2	Deployment Procedures, Supported Releases, and Core Components Deployed	22-2
22.3	Provisioning Oracle Application Server 10g Release 1 (10.1.3).....	22-2
22.3.1	Cloning a Running Oracle Application Server Instance	22-2
22.3.1.1	Cloning from an Existing Cluster, Scaling Up the Existing Cluster, and Using the Same Internet Directory 22-3	
22.3.1.1.1	Prerequisites	22-3
22.3.1.1.2	Provisioning Procedure	22-4
22.3.1.2	Provisioning from an Existing Cluster and Creating a New Cluster Without Internet Directory 22-8	
22.3.1.2.1	Prerequisites	22-8
22.3.1.2.2	Provisioning Procedure	22-9
22.3.1.3	Provisioning from an Existing Cluster and Creating a New Cluster With Internet Directory 22-13	
22.3.1.3.1	Prerequisites	22-13
22.3.1.3.2	Provisioning Procedure	22-14
22.3.2	Provisioning a Gold Image of the Oracle Application Server.....	22-18
22.3.2.1	Provisioning and Creating a New Cluster Without Internet Directory	22-18
22.3.2.1.1	Prerequisites	22-19
22.3.2.1.2	Provisioning Procedure	22-19
22.3.2.2	Provisioning and Creating a New Cluster With Internet Directory	22-24
22.3.2.2.1	Prerequisites	22-24
22.3.2.2.2	Provisioning Procedure	22-25
22.3.2.3	Provisioning and Treating Oracle Application Server as a Standalone Instance Without Internet Directory 22-29	
22.3.2.3.1	Prerequisites	22-29
22.3.2.3.2	Provisioning Procedure	22-30
22.3.2.4	Provisioning and Treating Oracle Application Server as a Standalone Instance With Internet Directory 22-34	
22.3.2.4.1	Prerequisites	22-34
22.3.2.4.2	Provisioning Procedure	22-35
22.4	Provisioning Oracle SOA Suite 10g (10.1.3.4 and 10.1.3.5)	22-39

Part VI Bare Metal Server Provisioning

23 Provisioning Bare Metal Servers

23.1	Getting Started with Provisioning Bare Metal Servers.....	23-1
23.2	Understanding Bare Metal Provisioning.....	23-2
23.2.1	Overview of the Bare Metal Provisioning Environment	23-2
23.2.2	Overview of the Bare Metal Provisioning Process.....	23-3
23.3	Supported Releases of Linux.....	23-4
23.4	Setting Up Infrastructure for Bare Metal Provisioning	23-4
23.4.1	Setting Up Stage Server.....	23-4
23.4.2	Setting Up Boot Server and DHCP Server	23-5
23.4.3	Setting Up RPM Repository	23-7
23.4.3.1	Setting UP RHEL 4 RPM Repository	23-7
23.4.3.2	Setting Up Oracle Linux 4 RPM Repository	23-8
23.4.3.3	Setting Up RHEL 5/Oracle Linux 5 RPM Repository.....	23-8
23.4.3.4	Exposing RPM Repository through HTTP or FTP	23-9
23.4.4	Configuring Stage Server.....	23-9
23.4.5	Configuring Boot Server	23-10
23.4.6	Configuring DHCP Server	23-11
23.4.7	Configuring RPM Repository	23-11
23.4.8	Checklist for Boot Server, Stage Server, RPM Repository, and Reference Host....	23-11
23.4.9	Configuring Software Library.....	23-12
23.4.9.1	Creating Operating System Component.....	23-12
23.4.9.2	Creating Disk Layout Component.....	23-14
23.4.10	Creating an Oracle Virtual Server Component	23-15
23.5	Provisioning Bare Metal Servers.....	23-16
23.5.1	Prerequisites	23-17
23.5.2	Procedure	23-17

Part VII Patch Management

24 Patching Software Deployments

24.1	Overview of the New Patch Management Solution	24-1
24.1.1	Overview of the Current Patch Management Challenges.....	24-1
24.1.2	Introduction to the New Patch Management Solution	24-2
24.1.3	Overview of Patch Plans.....	24-3
24.1.3.1	Introduction to Patch Plans.....	24-3
24.1.3.2	Types of Patch Plans	24-5
24.1.3.3	Introduction to Create Plan Wizard	24-5
24.1.4	Overview of Patch Templates	24-7
24.1.4.1	Introduction to Patch Templates.....	24-7
24.1.4.2	Introduction to Edit Template Wizard.....	24-7
24.1.5	Supported Targets, Releases, and Deployment Procedures.....	24-8
24.1.6	Supported Patching Modes	24-10
24.1.6.1	Patching in Online and Offline Mode.....	24-10
24.1.6.2	Patching in In-Place and Out-of-Place Mode	24-10
24.1.6.3	Patching in Rolling and Parallel Mode.....	24-12
24.1.7	Understanding the Patching Workflow	24-13

24.2	Setting Up Infrastructure for Patching	24-14
24.2.1	Meeting Basic Infrastructure Requirements	24-14
24.2.2	Creating Administrators with the Required Roles	24-14
24.2.3	Setting Up Infrastructure for Patching in Online Mode (Connected to MOS)	24-15
24.2.3.1	Enabling Online Mode	24-15
24.2.3.2	Setting Up Network Proxy and Realm Configuration Settings	24-16
24.2.4	Setting Up Infrastructure for Patching in Offline Mode (Not Connected to MOS)	24-17
24.2.4.1	Enabling Offline Mode	24-17
24.2.4.2	Downloading Enterprise Manager Catalog Zip File From Another Host With Internet Connectivity 24-17	
24.2.4.3	Uploading Enterprise Manager Catalog Zip File from your Host With No Internet Connectivity 24-18	
24.2.4.4	Creating "Refresh From My Oracle Support" Job	24-18
24.2.4.5	Uploading OPatch Patches to Oracle Software Library	24-19
24.2.4.6	Uploading Patches to Oracle Software Library	24-20
24.2.4.6.1	Downloading a Patch from My Oracle Support and Identifying the Details Required for Uploading a Patch to Software Library 24-21	
24.2.4.6.2	Uploading a Patch to the Software Library	24-22
24.2.5	Analyzing the Environment and Identifying Whether Your Targets Can Be Patched	24-24
24.2.5.1	Workarounds for Missing Property Errors	24-24
24.2.5.2	Workarounds for Unsupported Configuration Errors	24-25
24.3	Identifying Patches to Be Applied	24-26
24.3.1	(Online) Using Patch Recommendations	24-26
24.3.2	(Online) Using Knowledge Articles	24-28
24.3.3	(Online) Using Service Requests	24-28
24.3.4	(Online) Searching Patches on My Oracle Support	24-28
24.3.5	(Offline) Searching Patches in Oracle Software Library	24-29
24.4	Applying Patches	24-30
24.4.1	Creating a Patch Plan	24-30
24.4.2	Accessing the Patch Plan	24-31
24.4.3	Analyzing, Preparing, and Deploying Patch Plans	24-32
24.4.4	Switching Back to the Original Oracle Home After Deploying a Patch Plan	24-37
24.4.5	Saving Successfully Analyzed or Deployed Patch Plan As a Patch Template	24-38
24.4.6	(Optional) Creating a Patch Plan from a Patch Template and Applying Patches	24-38
24.4.7	Patching Oracle Exadata	24-39
24.4.7.1	Exadata Out-Of-Place Patching Of Oracle Grid Infrastructure and Oracle RAC Targets 24-41	
24.5	Diagnosing and Resolving Patching Issues	24-42
24.5.1	Diagnosing Patching Issues	24-42
24.5.2	Resolving Patching Issues	24-43
24.5.3	Rolling Back Patches	24-44
24.6	Additional Tasks You Can Perform	24-45
24.6.1	Viewing or Modifying Patch Template	24-45
24.6.2	Saving a Deployed Patch Plan as a Patch Template	24-45
24.6.3	Creating a Compliance Standard from a Patch Template	24-47
24.6.4	Downloading Patches from Patch Template	24-48

24.6.5	Deleting Patch Plan	24-48
24.6.6	Deleting Patch Template.....	24-48
24.6.7	Converting Nondeployable Patch Plan to Deployable Patch Plan	24-48
24.6.8	Associating Additional Targets to a Patch in a Patch Plan.....	24-49
24.6.9	Resolving Patch Conflicts	24-50
24.6.10	Analyzing the Results of Patching Operations.....	24-50
24.6.11	Customizing Patching Deployment Procedure.....	24-50
24.6.12	Patching Primary and Standby Databases Configured with Oracle Data Guard .	24-51
24.6.12.1	Overview of Patching Primary and Standby Databases.....	24-52
24.6.12.2	Patching Primary and Standby Databases.....	24-52
24.6.12.3	Customizing Patching deployment procedure	24-52
24.6.13	Rolling Back Patches	24-55

25 Patching Linux Hosts

25.1	Overview of Patching Linux Hosts	25-1
25.2	Understanding the Deployment Procedure for Patching Linux Hosts.....	25-2
25.3	Supported Linux Releases	25-2
25.4	Setting Up Infrastructure for Linux Patching	25-3
25.4.1	Meeting Prerequisites for Using the Linux Patching Feature	25-3
25.4.2	Setting Up the RPM Repository.....	25-4
25.4.2.1	Prerequisites for Setting Up the RPM Repository	25-4
25.4.2.2	Setting Up the RPM Repository	25-5
25.4.3	Setting Up Linux Patching Group for Compliance Reporting.....	25-6
25.4.3.1	Prerequisites for Setting Up Linux Patching Group.....	25-6
25.4.3.2	Setting Up a Linux Patching Group.....	25-6
25.5	Patching Linux Hosts	25-7
25.6	About Linux Patching Home Page.....	25-8
25.6.1	Viewing Compliance History	25-8
25.6.1.1	Prerequisites for Viewing Compliance History	25-8
25.6.1.2	Viewing Compliance History	25-9
25.6.2	Patching Non-Compliant Packages	25-9
25.6.2.1	Prerequisites for Patching Non-Compliant Packages	25-9
25.6.2.2	Patching Non-Compliant Packages	25-9
25.6.3	Rolling Back or Deinstalling Packages	25-10
25.6.3.1	Prerequisites for Deinstalling Packages	25-10
25.6.3.2	Rolling Back or Deinstalling Packages	25-10
25.6.4	Registering a Custom Channel	25-10
25.6.4.1	Prerequisites for Registering a Custom Channel.....	25-11
25.6.4.2	Registering a Custom Channel.....	25-11
25.6.5	Cloning a Channel	25-11
25.6.5.1	Prerequisites for Cloning a Channel.....	25-11
25.6.5.2	Cloning a Channel.....	25-12
25.6.6	Copying Packages from One Channel to Another	25-12
25.6.6.1	Prerequisites for Copying Packages from One Channel to Another	25-12
25.6.6.2	Copying Packages from One Channel to Another	25-12
25.6.7	Adding Custom Packages to a Channel.....	25-13
25.6.7.1	Prerequisites for Adding Custom Packages to a Channel.....	25-13

25.6.7.2	Adding Custom Packages to a Channel.....	25-13
25.6.8	Deleting a Channel	25-13
25.6.8.1	Prerequisites for Deleting a Channel	25-14
25.6.8.2	Deleting a Channel	25-14
25.7	About Configuration File Management	25-14
25.7.1	Prerequisites for Managing Configuration File.....	25-14
25.7.2	Creating Configuration File Channel.....	25-14
25.7.3	Uploading Configuration Files	25-15
25.7.3.1	Prerequisites for Uploading Configuration Files.....	25-15
25.7.3.2	Uploading Configuration Files.....	25-15
25.7.4	Importing Configuration Files	25-15
25.7.4.1	Prerequisites for Importing Configuration Files.....	25-15
25.7.4.2	Importing Configuration Files.....	25-15
25.7.5	Deploying Configuration Files	25-16
25.7.5.1	Prerequisites for Deploying Configuration Files	25-16
25.7.5.2	Deploying Configuration Files	25-16
25.7.6	Deleting Configuration File Channels	25-16
25.7.6.1	Prerequisites for Deleting Configuration File Channels.....	25-17
25.7.6.2	Deleting Configuration File Channels.....	25-17

Part VIII Configuration, Compliance, and Change Management

26 Managing Configuration Information

26.1	Overview of Configuration Management	26-1
26.2	Overview of Configuration Searches	26-3
26.2.1	Managing Configuration Searches	26-4
26.2.2	Setting Up a Search.....	26-4
26.2.3	Reviewing Search Scenarios.....	26-6
26.3	Overview of Configuration Browser.....	26-7
26.3.1	Viewing Configuration Data	26-8
26.3.2	Working with Saved Configurations	26-9
26.3.3	Working with Inventory and Usage Details	26-10
26.4	Overview of Configuration History	26-11
26.4.1	Accessing Configuration History	26-12
26.4.2	Working with Configuration History	26-12
26.4.2.1	Searching History	26-12
26.4.2.2	Annotating Configuration Changes	26-14
26.4.2.3	Scheduling a History Search and Creating a Notification List	26-14
26.4.2.4	Saving History to a File.....	26-15
26.4.3	Viewing History Job Activity	26-15
26.5	Overview of Comparisons and Templates.....	26-15
26.5.1	About Comparison Templates.....	26-15
26.5.2	Working with Comparison Templates	26-16
26.5.2.1	Creating or Editing a Comparison Template	26-16
26.5.2.2	Managing Comparison Templates.....	26-17
26.5.3	Specifying Rules.....	26-19

26.5.3.1	Creating a Value Constraint Rule	26-19
26.5.3.2	Creating a Matching Rule.....	26-19
26.5.3.3	Creating an Ignore Rule.....	26-20
26.5.4	About Rules Expression and Syntax	26-20
26.5.5	Understanding Rules by Example.....	26-22
26.5.5.1	Matching Rule Examples.....	26-22
26.5.5.2	Ignore Rule Examples	26-23
26.5.6	About Comparisons	26-24
26.5.7	Understanding the Comparison Wizard.....	26-25
26.5.7.1	Selecting a Configuration to Compare Against	26-25
26.5.7.2	Selecting Configurations to Compare	26-26
26.5.7.3	Selecting a Template to Use in the Comparison	26-26
26.5.7.4	Mapping Members in a System Comparison.....	26-26
26.5.7.5	Scheduling the Comparison and Creating a Notification List.....	26-27
26.5.7.6	Reviewing the Comparison Parameters and Submitting the Job.....	26-27
26.5.8	Working with Comparison Results.....	26-28
26.5.8.1	About Comparisons and Job Activity	26-28
26.5.8.2	About System Comparison Results	26-29
26.5.8.3	About Standard Target Comparison Results	26-29
26.5.8.4	Synchronizing Configuration Files	26-31
26.6	Overview of Custom Configurations and Collections	26-32
26.6.1	Working with Custom Configurations.....	26-33
26.6.1.1	Creating or Editing a Custom Configuration.....	26-33
26.6.1.2	Using the Files & Commands Tab.....	26-34
26.6.1.3	Using the SQL Tab.....	26-35
26.6.1.4	Setting Up Credentials.....	26-36
26.6.1.5	Setting Up Rules	26-36
26.6.1.6	Managing Custom Configurations	26-37
26.6.1.7	About Custom Configurations and Versioning.....	26-38
26.6.1.8	About Custom Configurations and Privileges.....	26-39
26.6.2	About Custom Configurations and Deployment.....	26-39
26.6.2.1	Deploying and Undeploying Custom Configurations	26-40
26.6.2.2	Editing a Deployment.....	26-41
26.6.2.3	Viewing a Configuration Collection.....	26-41
26.6.3	Extending Configuration Data Collections	26-41
26.6.3.1	Extending Existing Target Collections	26-42
26.6.3.2	Adding New Target Data Collections	26-42
26.6.4	Using Custom Configurations as Blueprints.....	26-43
26.7	Overview of Parsers	26-44
26.7.1	Managing Parsers	26-44
26.7.2	About XML Parsers	26-45
26.7.2.1	About the Default XML Parser.....	26-45
26.7.2.2	About the Generic XML Parser	26-46
26.7.2.3	XML Parser Examples.....	26-47
26.7.3	About Format-Specific Parsers	26-48
26.7.3.1	Database Query Parser Parameters	26-49
26.7.3.2	Directory Parser Parameters	26-50

26.7.3.3	E-Business Suite Parser Parameters	26-50
26.7.3.4	Galaxy CFG Parser Parameters	26-50
26.7.3.5	MQ-Series Parser Parameters	26-51
26.7.3.6	Siebel Parser Parameters	26-51
26.7.3.7	Unix Installed Patches Parser Parameters	26-51
26.7.3.8	Unix Recursive Directory List Parser Parameters	26-51
26.7.4	About Columnar Parsers	26-52
26.7.4.1	Columnar Parser Parameters	26-53
26.7.5	About Properties Parsers	26-54
26.7.5.1	Basic Properties Parser Parameters	26-55
26.7.5.2	Advanced Properties Parser Parameters	26-56
26.7.5.3	Advanced Properties Parser Constructs	26-57
26.7.6	Using Parsed Files and Rules	26-61
26.7.6.1	Sample XML File Parsing and Rule Application	26-61
26.7.6.2	Sample Non-XML File Parsing and Rule Application	26-63
26.7.6.3	Sample SQL Query Parsing and Rule Application	26-65
26.8	Overview of Client Configurations	26-66
26.8.1	About Client System Analyzer in Cloud Control	26-67
26.8.2	Deploying Client System Analyzer Independently	26-67
26.9	Overview of Relationships	26-68
26.10	Overview of Configuration Topology Viewer	26-69
26.10.1	About Configuration Topology Viewer	26-70
26.10.2	Examples of Using Topology	26-70
26.10.3	Viewing a Configuration Topology	26-70
26.10.4	Determining System Component Structure	26-71
26.10.5	Determining General Status of Target's Configuration Health	26-71
26.10.6	Getting Configuration Health/Compliance Score of a Target	26-72
26.10.7	Analyzing a Problem and Viewing a Specific Issue in Detail	26-72
26.10.8	About Dependency Analysis	26-73
26.10.9	About Impact Analysis	26-73
26.10.10	Creating a Custom Topology View	26-73
26.10.11	Deleting a Custom Topology View	26-74
26.10.12	Excluding Relationships from a Custom Topology View	26-74
26.10.13	Including Relationships to a Target in a Custom Topology View	26-74
26.10.14	Creating a Relationship to a Target	26-75
26.10.15	Deleting a Relationship from a Target	26-75
26.10.16	Controlling the Appearance of Information on a Configuration Topology Graph	26-76

27 Managing Compliance

27.1	Overview of Compliance	27-1
27.1.1	Terminology Used in Compliance	27-2
27.1.2	Accessing the Compliance Features	27-4
27.1.3	Privileges and Roles Needed to Use the Compliance Features	27-4
27.2	Evaluating Compliance	27-5
27.2.1	Accessing Compliance Statistics	27-7
27.2.1.1	Using the Compliance Dashboard Effectively	27-7

27.2.2	Viewing Compliance Summary Information	27-8
27.2.3	Viewing Target Compliance Evaluation Results	27-8
27.2.4	Viewing Compliance Framework Evaluation Results	27-9
27.2.5	Investigating Compliance Violations and Evaluation Results.....	27-10
27.2.5.1	Investigating Violations of Repository Compliance Standard Rules and Targets Causing Violations 27-10	
27.2.5.2	Viewing All the Violations Reported for Your Enterprise	27-11
27.2.5.3	Examples of Viewing Violations	27-11
27.2.6	Investigating Evaluation Errors.....	27-14
27.2.7	Analyzing Compliance Reports.....	27-15
27.2.8	Overview of Compliance Score and Importance	27-16
27.2.8.1	Compliance Score of a Compliance Standard Rule -Target	27-16
27.2.8.2	Real-time Monitoring Rule Compliance Score.....	27-17
27.2.8.3	Compliance Score of a Compliance Standard for a Target.....	27-17
27.2.8.4	Compliance Framework Compliance Score	27-18
27.2.8.5	Parent Node Compliance Score.....	27-18
27.3	Investigating Real-time Observations.....	27-19
27.3.1	Viewing Observations.....	27-19
27.3.1.1	Viewing Observations By Systems	27-19
27.3.1.2	Viewing Observations By Compliance Framework	27-20
27.3.1.3	Viewing Observations By Search	27-21
27.3.1.4	Viewing Details of an Incident	27-21
27.3.2	Operations on Observations During Compliance Evaluation	27-22
27.3.2.1	Manually Setting an Observation As Authorized Or Not Authorized	27-22
27.3.2.2	Notifying a User When an Observation Occurs	27-23
27.3.2.3	Notifying a User When an Authorized Observation Occurs	27-23
27.4	Configuring Compliance Management	27-23
27.4.1	About Compliance Frameworks	27-24
27.4.2	Operations on Compliance Frameworks	27-26
27.4.2.1	Creating a Compliance Framework.....	27-26
27.4.2.2	Creating Like a Compliance Framework	27-28
27.4.2.3	Editing a Compliance Framework	27-28
27.4.2.4	Deleting a Compliance Framework	27-29
27.4.2.5	Exporting a Compliance Framework	27-29
27.4.2.6	Importing a Compliance Framework	27-30
27.4.2.7	Browsing Compliance Frameworks.....	27-30
27.4.2.8	Searching Compliance Frameworks	27-30
27.4.2.9	Browsing Compliance Framework Evaluation Results	27-30
27.4.2.10	Searching Compliance Framework Evaluation Results.....	27-31
27.4.2.11	Browsing Compliance Framework Errors	27-31
27.4.2.12	Searching Compliance Framework Errors.....	27-31
27.4.2.13	Verifying Database Targets Are Compliant with Compliance Frameworks..	27-32
27.4.3	About Compliance Standards.....	27-32
27.4.4	Operations on Compliance Standards.....	27-34
27.4.4.1	Creating a Compliance Standard	27-35
27.4.4.2	Creating Like a Compliance Standard	27-37
27.4.4.3	Editing a Compliance Standard	27-37
27.4.4.4	Deleting a Compliance Standard	27-38

27.4.4.5	Exporting a Compliance Standard	27-38
27.4.4.6	Importing a Compliance Standard	27-38
27.4.4.7	Browsing Compliance Standards	27-39
27.4.4.8	Searching Compliance Standards	27-39
27.4.4.9	Browsing Compliance Standard Evaluation Results	27-39
27.4.4.10	Searching Compliance Standard Evaluation Results	27-40
27.4.4.11	Browsing Compliance Standard Errors.....	27-40
27.4.4.12	Searching Compliance Standard Errors	27-40
27.4.4.13	Associating a Compliance Standard with Targets.....	27-41
27.4.4.14	Viewing Real-time Monitoring Compliance Standard Warnings	27-42
27.4.4.15	Enabling Security Metrics	27-42
27.4.4.16	Considerations When Creating Compliance Standards	27-43
27.4.5	About Compliance Standard Rule Folders	27-43
27.4.5.1	Creating Rule Folders	27-43
27.4.5.2	Managing Rule Folders in a Compliance Standard.....	27-44
27.4.6	About Compliance Standard Rules.....	27-44
27.4.7	Operations on Compliance Standards Rules	27-45
27.4.7.1	Creating a Repository Compliance Standard Rule.....	27-45
27.4.7.2	Creating a WebLogic Server Signature Compliance Standard Rule.....	27-47
27.4.7.3	Creating a Real-time Monitoring Compliance Standard Rule.....	27-52
27.4.7.4	Creating Like a Compliance Standard Rule	27-58
27.4.7.5	Editing a Compliance Standard Rule	27-58
27.4.7.6	Deleting a Compliance Standard Rule	27-59
27.4.7.7	Exporting a Compliance Standard Rule.....	27-59
27.4.7.8	Importing a Compliance Standard Rule	27-60
27.4.7.9	Browsing Compliance Standard Rules.....	27-60
27.4.7.10	Searching Compliance Standard Rules	27-60
27.4.7.11	Compliance Standard Rules Provided by Oracle	27-60
27.5	Real-time Monitoring Facets	27-61
27.5.1	About Real-time Monitoring Facets	27-61
27.5.1.1	Facet Entity Types	27-62
27.5.1.2	Facet Patterns	27-62
27.5.2	Operations on Facets	27-63
27.5.2.1	Viewing the Facet Library	27-63
27.5.2.2	Creating and Editing Facets.....	27-64
27.5.2.3	Creating and Editing Facet Folders	27-66
27.5.2.4	Deleting a Facet.....	27-66
27.5.2.5	Using Create Like to Create a New Facet	27-67
27.5.2.6	Importing and Exporting Facets.....	27-67
27.5.2.7	Changing Base Facet Attributes Not Yet Used In a Rule.....	27-68
27.6	Example of Creating Repository Rule Based on Custom Configuration Collections..	27-69

28 Managing Database Configuration Changes

28.1	Overview of Change Management for Databases	28-1
28.2	Overview of Schema Baselines	28-2
28.2.1	Overview of Scope Specification	28-3
28.2.2	Capturing a Schema Baseline Version	28-4

28.2.3	Working With A Schema Baseline Version.....	28-5
28.2.4	Working With Multiple Schema Baseline Versions.....	28-6
28.2.5	Exporting and Importing Schema Baselines.....	28-8
28.2.5.1	Creating Directory Objects for Export and Import.....	28-8
28.3	Overview of Schema Comparisons	28-9
28.3.1	Defining Schema Comparisons	28-10
28.3.2	Working with Schema Comparison Versions	28-12
28.4	Overview of Schema Synchronizations	28-13
28.4.1	Defining Schema Synchronizations	28-14
28.4.2	Creating a Synchronization Definition from a Comparison	28-17
28.4.3	Working with Schema Synchronization Versions	28-17
28.4.3.1	The Schema Synchronization Cycle.....	28-17
28.4.4	Creating Additional Synchronization Versions	28-23
28.5	Overview of Change Plans	28-23
28.5.1	Working with Change Plans	28-24
28.5.2	Creating a Change Plan	28-24
28.5.2.1	Creating and Applying a Change Plan From a Schema Comparison	28-25
28.5.2.1.1	Prerequisites to Creating a Change Plan	28-25
28.5.2.1.2	Creating a Change Plan.....	28-25
28.5.2.1.3	Applying a Change Plan	28-27
28.5.2.2	Using External Clients to Create and Access Change Plans in Cloud Control	28-27
28.5.2.2.1	Setting Up Cloud Control Administrator For Change Plans.....	28-28
28.5.3	Submitting Schema Change Plans From SQL Developer Interface	28-28
28.6	Overview of Data Comparison	28-29
28.6.1	Requirements for Data Comparisons	28-29
28.6.2	Comparing Data and Viewing Results	28-31

29 Additional Setup for Real-time Monitoring

29.1	Overview of Real-Time Monitoring	29-1
29.2	Overview of Resource Consumption Considerations	29-2
29.2.1	OS File Monitoring Archiving	29-2
29.2.2	OS File Read Monitoring	29-2
29.2.3	Creating Facets That Have Very Broad Coverage	29-2
29.2.4	Cloud Control Repository Sizing	29-3
29.3	Configuring Monitoring Credentials	29-3
29.4	Preparing To Monitor Linux Hosts	29-4
29.4.1	OS File Monitoring	29-4
29.4.2	Debugging Kernel Module Or Other File Monitoring Issues	29-6
29.5	Preparing To Monitor Windows Hosts	29-7
29.5.1	Verifying Auditing Is Configured Properly	29-8
29.5.2	Subinacl External Requirements.....	29-8
29.6	Preparing To Monitor Solaris Hosts.....	29-9
29.6.1	Enabling BSM Auditing	29-9
29.6.1.1	Using Solaris Versions 9 and 10	29-9
29.6.1.2	Using Solaris 11.....	29-10
29.6.2	Managing Audit Log Files.....	29-10

29.7	Preparing to Monitor AIX Hosts.....	29-11
29.7.1	Installation Prerequisite for AIX 5.3.....	29-11
29.7.2	Administering AIX Auditing	29-11
29.7.3	Verifying AIX System Log Files for the OS User Monitoring Module	29-12
29.8	Preparing To Monitor the Oracle Database	29-12
29.8.1	Setting Auditing User Privileges	29-12
29.8.2	Specifying Audit Options.....	29-12
29.9	Setting Up Change Request Management Integration.....	29-14
29.9.1	BMC Remedy Action Request System 7.1 Integration.....	29-14
29.9.1.1	Remedy Installation and Customization	29-14
29.9.1.1.1	Adding the Connector to Cloud Control 29-16	
29.9.1.1.2	Using Automatic Reconciliation Rules.....	29-18
29.9.1.1.3	Creating Change Requests for Upcoming Changes.....	29-18
29.9.1.1.4	Overview of Reconciliation Functionality	29-19
29.10	Overview of the Repository Views Related to Real-time Monitoring Features	29-20
29.11	Modifying Data Retention Periods.....	29-25
29.12	Real-time Monitoring Supported Platforms	29-25
29.12.1	OS User Monitoring	29-25
29.12.2	OS Process Monitoring.....	29-27
29.12.3	OS File Monitoring	29-28
29.12.4	OS Windows Registry Monitoring.....	29-30
29.12.5	OS Windows Active Directory User Monitoring.....	29-30
29.12.6	OS Windows Active Directory Computer Monitoring.....	29-30
29.12.7	OS Windows Active Directory Group Monitoring.....	29-31
29.12.8	Oracle Database Table Monitoring	29-31
29.12.9	Oracle Database View Monitoring.....	29-32
29.12.10	Oracle Database Materialized View Monitoring	29-32
29.12.11	Oracle Database Index Monitoring	29-33
29.12.12	Oracle Database Sequence Monitoring.....	29-33
29.12.13	Oracle Database Procedure Monitoring.....	29-33
29.12.14	Oracle Database Function Monitoring	29-33
29.12.15	Oracle Database Package Monitoring.....	29-34
29.12.16	Oracle Database Library Monitoring.....	29-34
29.12.17	Oracle Database Trigger Monitoring	29-34
29.12.18	Oracle Database Tablespace Monitoring.....	29-35
29.12.19	Oracle Database Cluster Monitoring	29-35
29.12.20	Oracle Database Link Monitoring	29-35
29.12.21	Oracle Database Dimension Monitoring.....	29-35
29.12.22	Oracle Database Profile Monitoring	29-36
29.12.23	Oracle Database Public Link Monitoring.....	29-36
29.12.24	Oracle Database Public Synonym Monitoring.....	29-36
29.12.25	Oracle Database Synonym Monitoring	29-36
29.12.26	Oracle Database Type Monitoring	29-37
29.12.27	Oracle Database Role Monitoring	29-37
29.12.28	Oracle Database User Monitoring.....	29-37
29.12.29	Oracle Database SQL Query Statement Monitoring.....	29-38

Part IX Oracle Site Guard

30 Using Oracle Site Guard

30.1	New Features of Oracle Site Guard in Enterprise Manager Cloud Control 12c Release 2.....	30-1
30.1.1	User Interface for Creating Oracle Site Guard Configuration	30-1
30.1.2	Preferred Credential Support.....	30-2
30.1.3	Re-Order Execution Order	30-2
30.2	Important Notes Before You Begin	30-2
30.3	Overview of Oracle Site Guard.....	30-3
30.3.1	Benefits of Oracle Site Guard	30-3
30.3.2	Oracle Site Guard Operations	30-4
30.3.3Site Representation in Enterprise Manager Cloud Control	30-4
30.4	Terminology Used in Oracle Site Guard	30-6
30.5	Using Oracle Site Guard: Task Overview	30-7
30.5.1	Task Overview	30-7
30.5.2	Task Roadmap.....	30-8
30.6	Installing Oracle Site Guard	30-10
30.7	Prerequisites for Configuring Oracle Fusion Middleware Products for Oracle Site Guard....	30-11
30.7.1	Discovering Targets on the Primary Site and the Standby Site	30-11
30.7.2	Creating Generic Systems for the Primary and Standby Sites	30-12
30.7.2.1	Using Enterprise Manager Cloud Control Console to Create a Generic System.....	30-12
30.7.2.2	Using EMCLI Commands to Create a Generic System.....	30-13
30.7.3	Creating Credentials.....	30-14
30.7.4	Configuring the Software Library	30-16
30.8	Configuring Oracle Site Guard	30-17
30.8.1	Configuring Sites Using Generic Systems.....	30-20
30.8.1.1	Configuring Sites Using Enterprise Manager Cloud Control Console	30-20
30.8.1.2	Configuring Sites Using EMCLI Commands	30-20
30.8.2	Associating Credentials	30-21
30.8.2.1	Associating Credentials Using Enterprise Manager Cloud Control Console	30-21
30.8.2.2	Associating Credentials Using EMCLI Commands	30-22
30.8.3	Associating Pre-Scripts and Post-Scripts.....	30-23
30.8.3.1	Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console	30-23
30.8.3.2	Associating Pre-Scripts and Post-Scripts Using EMCLI Commands	30-24
30.8.4	Associating Storage Scripts	30-25
30.8.4.1	Associating Storage Scripts Using Enterprise Manager Cloud Control Console	30-25
30.8.4.2	Associating Storage Scripts Using EMCLI Commands	30-25
30.9	Executing Oracle Site Guard Operations.....	30-27
30.9.1	Creating an Operation Plan.....	30-27
30.9.2	Updating an Operation Plan.....	30-28
30.9.3	Running Precheck Utility	30-28
30.9.4	Submitting an Operation Plan	30-29
30.9.5	Monitoring an Operation Plan.....	30-29

30.10	Error Management Framework	30-30
30.10.1	Error Modes.....	30-30
30.10.1.1	Stop Error Mode	30-30
30.10.1.2 Continue Error Mode	30-31
30.10.2	Updating Error Modes in an Operation Plan	30-32
30.10.3	Retrying a Failed Operation.....	30-33
30.11	Managing a Site Using Oracle Site Guard.....	30-33
30.11.1	Stopping a Site.....	30-34
30.11.2	Starting a Site.....	30-34
30.11.3	Performing	Site Switchover 30-34
30.11.4	Performing	Site Failover 30-34

31 Example Scenario: Using Oracle Site Guard

31.1	Task 1: Setting Up Oracle Business Intelligence Enterprise Deployment	31-1
31.2	Task 2: Discovering Targets for the Primary Site and the Standby Site	31-2
31.3	Task 3: Creating Production and Standby Systems for Oracle Business Intelligence....	31-3
31.4	Task 4: Creating Credentials	31-4
31.5	Task 5: Configuring the Software Library	31-4
31.6	Task 6: Creating Oracle Site Guard Configuration	31-4
31.6.1	Associating Oracle Business Intelligence Sites Using Enterprise Manager Cloud Control Console	31-4
31.6.2	Associating Oracle Business Intelligence Sites Using EMCLI Commands	31-5
31.7	Task 7: Associating Credentials for Site.....	31-5
31.7.1	Associating Credentials for Oracle Business Intelligence Sites Using Enterprise Manager Cloud Control Console	31-5
31.7.2	Associating Credentials for Oracle Business Intelligence Sites Using EMCLI Commands	31-7
31.8	Task 8: Creating Pre-Scripts and Post-Scripts.....	31-9
31.8.1	Creating Pre-Scripts and Post-Scripts for Start or Stop Operations	31-9
31.8.2	Creating Pre-Scripts and Post-Scripts for Switchover or Failover Operations.....	31-12
31.9	Task 9: Associating Storage Scripts	31-16
31.9.1	Associating Storage Scripts for Oracle Business Intelligence Sites Using Enterprise Manager Cloud Control Console	31-16
31.9.2	Associating Storage Scripts for Oracle Business Intelligence Sites Using EMCLI Commands	31-18
31.10	Task 10: Creating Operation Plans	31-19
31.11	Task 11: Starting BISystem1.....	31-21
31.12	Task 12: Stopping BISystem1	31-22
31.13	Task 13: Running the Oracle Site Guard Pre-Check Utility	31-22
31.14	Task 14: Performing	Site Switchover 31-22
31.15	Task 15: Performing	Site Failover 31-23

Part X Deployment Procedures

32 About Deployment Procedures

32.1	Overview of the Procedure Management Solution	32-1
32.1.1	Overview of the Provisioning Page	32-1

32.1.2	Comparison Between the Existing Design and the New Design for Procedure Instance Execution Page	32-2
32.1.3	Overview of the New Procedure Instance Execution Page	32-4
32.2	Granting Roles and Privileges to Administrators	32-6
32.2.1	Granting Roles and Privileges to Administrators on the Deployment Procedure .	32-6
32.2.2	Granting Roles and Privileges to Administrators on Software Library	32-8
32.3	Components of a Procedure	32-8
32.3.1	Target List	32-9
32.3.2	Procedure Variables	32-9
32.3.3	Phases and Steps	32-10
32.4	Creating, Saving, and Launching User Defined Deployment Procedure (UDDP)	32-13
32.4.1	Step 1: Creating User Defined Deployment Procedure	32-13
32.4.2	Step 2: Saving and Launching User Defined Deployment Procedure with Default Inputs	32-14
32.4.2.1	Saving and Launching the Deployment Procedure with Lock Down.....	32-14
32.4.3	Step 3: Launching and Running the Saved User Defined Deployment Procedure	32-21
32.4.4	Step 4: Tracking the Submitted User Defined Deployment Procedure	32-21
32.5	Managing Deployment Procedures	32-21
32.5.1	Viewing, Editing, Deleting a Procedures	32-22
32.5.2	Editing and Saving Permissions of a Procedures.....	32-22
32.5.3	Tracking the Procedure Execution and Status of Deployment Procedures	32-22
32.6	Executing Procedure Instance Tasks.....	32-24
32.6.1	Investigating a Failed Step for a Single or a Set of Targets.....	32-24
32.6.2	Retrying a Failed Step	32-24
32.6.3	Creating an Incident.....	32-24
32.6.4	Viewing the Execution Time of a Deployment Procedure	32-25
32.6.5	Searching for a Step	32-25
32.6.6	Filtering the Failed Steps	32-25
32.6.7	Downloading a Step Output	32-25

33 Customizing Deployment Procedures

33.1	Understanding Customization Types.....	33-1
33.2	Customizing a Deployment Procedure	33-3
33.2.1	Adding Phases or Steps	33-3
33.2.1.1	Adding Rolling or Parallel Phase	33-3
33.2.1.2	Adding Job Step	33-4
33.2.1.3	Adding Directive Step	33-5
33.2.1.4	Adding Component Step.....	33-6
33.2.1.5	Adding File Transfer Step	33-7
33.2.1.6	Adding Host Command Step	33-7
33.2.1.7	Adding Manual Step	33-8
33.2.2	Adding Target Lists.....	33-9
33.2.3	Adding Procedure Variables.....	33-9
33.2.4	Deleting Phases or Steps	33-9
33.2.5	Enabling or Disabling Phases or Steps	33-10
33.3	Editing a Custom Deployment Procedure	33-10

33.4	Changing Error Handling Modes.....	33-11
33.5	Setting Up E-Mail Notifications.....	33-12
33.5.1	Configuring an Outgoing Mail (SMTP) Server Within Enterprise Manager.....	33-12
33.5.2	Providing the Administrator Enterprise Manager E-mail and Password.....	33-14
33.6	Copying Customized Provisioning Entities from One Enterprise Manager Site to Another..	33-14
33.7	Customizing Directive WorkFlow Example.....	33-15
33.7.1	Creating and Uploading Copy of a Default Directive.....	33-16
33.7.2	Customizing Deployment Procedure to Use the New Directive.....	33-16
33.7.3	Running the Customized Deployment Procedure	33-17

Part XI Additional Information

A Using Enterprise Manager Command Line Interface

A.1	Overview	A-1
A.2	Prerequisites	A-2
A.3	Enterprise Manager Command Line Interface Verbs.....	A-2
A.3.1	Provisioning EM CLI Verbs	A-2
A.3.1.1	New Enterprise Manager Command Line Interface Verbs.....	A-2
A.3.1.2	Obsolete Enterprise Manager Command Line Interface Verbs.....	A-3
A.3.1.3	Enterprise Manager Command Line Interface Verbs for Running Procedures..	A-3
A.3.2	Patching EM CLI Verbs.....	A-6
A.3.3	Software Library EM CLI Verbs	A-9
A.4	Provisioning Using EM CLI	A-12
A.4.1	Creating the Properties File to Submit a Deployment Procedure	A-12
A.4.2	Using Properties File from an Existing Execution of a Deployment Procedure	A-15
A.4.3	Launching a Procedure using an Existing Saved Procedure.....	A-16
A.4.3.1	Saving a Procedure Configuration of a Procedure.....	A-17
A.4.3.2	Updating the Procedure Configuration of a Procedure.....	A-17
A.5	Patching Using EM CLI.....	A-17
A.5.1	Before You Begin.....	A-18
A.5.2	Patching Using EM CLI	A-18
A.5.2.1	Creating a New Properties File for Patching Targets.....	A-19
A.5.2.2	Using the Properties File of an Existing Patch Plan to Patch the targets.....	A-23
A.6	WorkFlow Examples Using EM CLI Commands	A-25
A.6.1	Provisioning Oracle Database Software	A-25
A.6.2	Provisioning Oracle WebLogic Server.....	A-26
A.6.3	Provisioning User Defined Deployment Procedure.....	A-30
A.6.3.1	Prerequisites	A-31
A.6.3.2	Adding Steps and Phases to User Defined Deployment Procedure Using GUI.....	A-31
A.6.3.3	Using EM CLI commands to Run an Instance of the Procedure	A-32
A.6.4	Patching WebLogic Server Target.....	A-32
A.6.5	Creating a New Generic Component by Associating a Zip File.....	A-36
A.6.5.1	Step 1: Identifying the Parent Folder in Software Library.....	A-37
A.6.5.2	Step 2: Creating a Genetic Component Entity.....	A-38
A.6.5.3	Step 3: Associating a Zip File to the Generic Component	A-40

A.6.5.4	Step 4: Verifying the Newly Created Entity	A-40
A.7	Limitations of Using Enterprise Manager Command Line Interface.....	A-40

B Checking Host Readiness

B.1	Setting Up User Accounts.....	B-1
B.1.1	Configuring SSH.....	B-2
B.2	Shell Limits	B-2
B.3	Root Setup (Privilege Delegation)	B-2
B.4	Environment Settings	B-2
B.4.1	Kernel Requirements.....	B-3
B.4.2	Node Time Requirements.....	B-3
B.4.3	Package Requirements	B-4
B.4.4	Memory and Disk Space Requirements	B-4
B.4.5	Network & IP Address Requirements	B-4
B.5	Storage Requirements	B-5
B.6	Installation Directories and Oracle Inventory	B-6

C Using emctl partool Utility

C.1	Overview of Provisioning Archive Files	C-1
C.2	Overview of emctl partool Utility	C-1
C.3	Checking Oracle Software Library	C-3
C.4	Exporting Deployment Procedures.....	C-3
C.4.1	Obtaining Deployment Procedure's GUID.....	C-3
C.4.2	Creating PAR File	C-4
C.5	Importing PAR Files	C-4
C.5.1	Importing Using Command Line Interface	C-5
C.5.1.1	Importing Specific PAR File.....	C-5
C.5.1.2	Importing All PAR Files	C-5
C.5.2	Importing Using Cloud Control Console.....	C-5

D Understanding PXE Booting and Kickstart Technology

D.1	About PXE Booting and Kickstart Technology	D-1
D.2	Subnet Provisioning Usecases.....	D-2

E Troubleshooting Issues

E.1	Troubleshooting Database Provisioning Issues	E-1
E.1.1	Grid Infrastructure Root Script Failure	E-1
E.1.2	SUDO Error During Deployment Procedure Execution.....	E-2
E.1.3	Prerequisites Checks Failure	E-2
E.1.4	Oracle Automatic Storage Management (Oracle ASM) Disk Creation Failure	E-2
E.1.5	Oracle ASM Disk Permissions Error.....	E-3
E.1.6	Specifying a Custom Temporary Directory for Database Provisioning.....	E-3
E.1.7	Incident Creation When Deployment Procedure Fails	E-3
E.1.8	Reading Remote Log Files	E-4
E.1.9	Retrying Failed Jobs	E-4
E.2	Troubleshooting Patching Issues.....	E-4

E.2.1	Oracle Software Library Configuration Issues.....	E-5
E.2.1.1	Error Occurs While Staging a File	E-5
E.2.1.2	Error Occurs While Uploading a Patch Set.....	E-5
E.2.1.3	OPatch Update Job Fails When Duplicate Directories Are Found in the Software Library E-5	
E.2.2	My Oracle Support Connectivity Issues.....	E-6
E.2.2.1	Error Occurs While Testing the Proxy Server That Supports Only Digest Authentication E-6	
E.2.3	Host and Oracle Home Credential Issues	E-7
E.2.3.1	Cannot Create Log Files When You Set Privileged Credentials as Normal Oracle Home Credentials E-8	
E.2.4	Collection Issues	E-9
E.2.4.1	Missing Details in Plan Wizard	E-9
E.2.4.2	Cannot Add Targets to a Patch Plan.....	E-10
E.2.5	Patch Recommendation Issues	E-11
E.2.5.1	Patch Recommendations Do Not Appear After Installing Oracle Management Agent on Oracle Exadata Targets E-11	
E.2.6	Patch Plan Issues.....	E-12
E.2.6.1	Patch Plan Becomes Nondeployable and Fails	E-12
E.2.6.2	Instances Not to Be Migrated Are Also Shown as Impacted Targets for Migration.. E-12	
E.2.6.3	Cluster ASM and Its Instances Do Not Appear as Impacted Targets While Patching a Clusterware Target E-13	
E.2.6.4	Recovering from a Partially Prepared Plan	E-14
E.2.6.5	Error #1009 Appears in the Create Plan Wizard While Creating or Editing a Patch Plan E-14	
E.2.6.6	Analysis Succeeds But the Deploy Button is Disabled	E-14
E.2.6.7	Patch Plan Fails When Patch Plan Name Exceeds 64 Bytes	E-15
E.2.6.8	Out-of-Place Patching Fails for 11.2.0.3 Exadata Clusterware.....	E-15
E.2.7	Patch Plan Analysis Issues	E-16
E.2.7.1	Patch Plan Remains in Analysis State Even After the Deployment Procedure Ends. E-16	
E.2.7.2	Patch Plan Analysis Fails When the Host's Node Name Property Is Missing. E-17	
E.2.7.3	Link to Show Detailed Progress on the Analysis Is Not Actionable.....	E-18
E.2.7.4	Raising Service Requests When You Are Unable to Resolve Analysis Failure Issues E-18	
E.2.8	User Account and Role Issues.....	E-19
E.2.8.1	Out-of-Place Patching Errors Out If Patch Designers and Patch Operators Do Not Have the Required Privileges E-19	
E.3	Troubleshooting Linux Patching Issues	E-19
E.4	Troubleshooting Linux Provisioning Issues	E-20
E.5	Troubleshooting Oracle Site Guard Issues.....	E-22
E.5.1	Operation Plan Failure.....	E-22
E.5.2	Switchover or Failover Operations Failure.....	E-24
E.5.3	Precheck Failure	E-25
E.5.4	Oracle WebLogic Server Failure.....	E-26
E.5.5	Database Failure.....	E-27
E.6	Frequently Asked Questions on Linux Provisioning	E-28

E.7	Refreshing Configurations.....	E-30
E.7.1	Refreshing Host Configuration.....	E-30
E.7.2	Refreshing Oracle Home Configuration.....	E-30
E.8	Reviewing Log Files	E-31
E.8.1	OMS-Related Log Files	E-31
E.8.2	Management Agent-Related Log Files	E-32
E.8.3	Advanced Options.....	E-32
E.8.3.1	On the OMS Side	E-32
E.8.3.2	On the Management Agent Side	E-32

F Oracle Site Guard Command-Line Interface Reference

F.1	add_siteguard_script_hosts.....	F-2
F.2	create_operation_plan	F-2
F.3	create_siteguard_configuration	F-3
F.4	create_siteguard_credential_association	F-3
F.5	create_siteguard_script	F-4
F.6	delete_operation_plan.....	F-5
F.7	delete_siteguard_configuration	F-6
F.8	delete_siteguard_credential_association	F-6
F.9	delete_siteguard_script	F-7
F.10	delete_siteguard_script_hosts.....	F-7
F.11	get_operation_plan_details	F-8
F.12	get_operation_plans	F-8
F.13	get_siteguard_configuration	F-9
F.14	get_siteguard_credential_association	F-9
F.15	get_siteguard_script_hosts	F-10
F.16	get_siteguard_scripts.....	F-10
F.17	run_prechecks.....	F-11
F.18	submit_operation_plan	F-11
F.19	update_operation_plan	F-12
F.20	update_siteguard_configuration	F-12
F.21	update_siteguard_credential_association	F-13
F.22	update_siteguard_script	F-14

Index

Preface

The Lifecycle Management Guide introduces you to the lifecycle management solutions offered by Oracle Enterprise Manager Cloud Control (Cloud Control), and describes in detail how you can use the discovery, provisioning, patching, and configuration and compliance management features to manage your data center.

Audience

This guide is primarily meant for administrators who want to use the discovery, provisioning, patching, and configuration and compliance management features offered by Cloud Control to meet their lifecycle management challenges. As an administrator, you can be either a *Designer*, who performs the role of a system administrator and does critical data center operations, or an *Operator*, who runs the default as well custom deployment procedures, patch plans, and patch templates to manage the enterprise configuration.

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 books in the Cloud Control documentation library:

- *Oracle Enterprise Manager Cloud Control Basic Install Guide*
- *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*
- *Oracle Enterprise Manager Cloud Control Upgrade Guide*
- *Oracle Enterprise Manager Cloud Control Administrator's Guide*

For the latest releases of these and other Oracle documentation, check the Oracle Technology Network at the following URL:

<http://www.oracle.com/technetwork/indexes/documentation/index.html>

Cloud Control also provides extensive online Help. Click **Help** at the top-right corner of any Cloud Control page to display the online help window.

Conventions

The following conventions are used in this document:

Convention	Meaning
boldface	Indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
<i>italic</i>	Indicates book titles, emphasis, or placeholder variables for which you supply particular values.
monospace	Indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.
Other Graphics	Graphics have been used extensively in addition to the textual descriptions to ensure that certain concepts and processes are illustrated better.

Part I

Overview and Setup Details

This part contains the following chapters:

- [Chapter 1, "Introduction to Lifecycle Management"](#)
- [Chapter 2, "Setting Up Your Infrastructure"](#)

Introduction to Lifecycle Management

This chapter covers the following:

- [Overview of the New Lifecycle Management Solutions](#)
- [Information Map](#)

1.1 Overview of the New Lifecycle Management Solutions

In today's world, with the cloud infrastructure, numerous low cost servers and software deployments on those servers have brought in a fresh set of lifecycle management challenges. The challenges range from discovering and monitoring the health of existing software deployments to provisioning new software deployments and maintaining them over a period of time.

Besides that, other problems include difficulty in managing consistency and compatibility across these software deployments and operating systems, managing configuration changes, and managing security vulnerabilities that lead to lack of compliance.

These lifecycle management challenges eventually force you to engage more human resources and devote significant amount of time in managing the data center operations.

Oracle Enterprise Manager Cloud Control (Cloud Control) offers lifecycle management solutions that help you meet all lifecycle management challenges easily by automating time-consuming tasks related to discovery, initial provisioning and cloning, patching, configuration management, ongoing change management, and compliance management.

[Figure 1-1](#) illustrates the lifecycle management solutions offered by Cloud Control.

Figure 1–1 Lifecycle Management Solutions

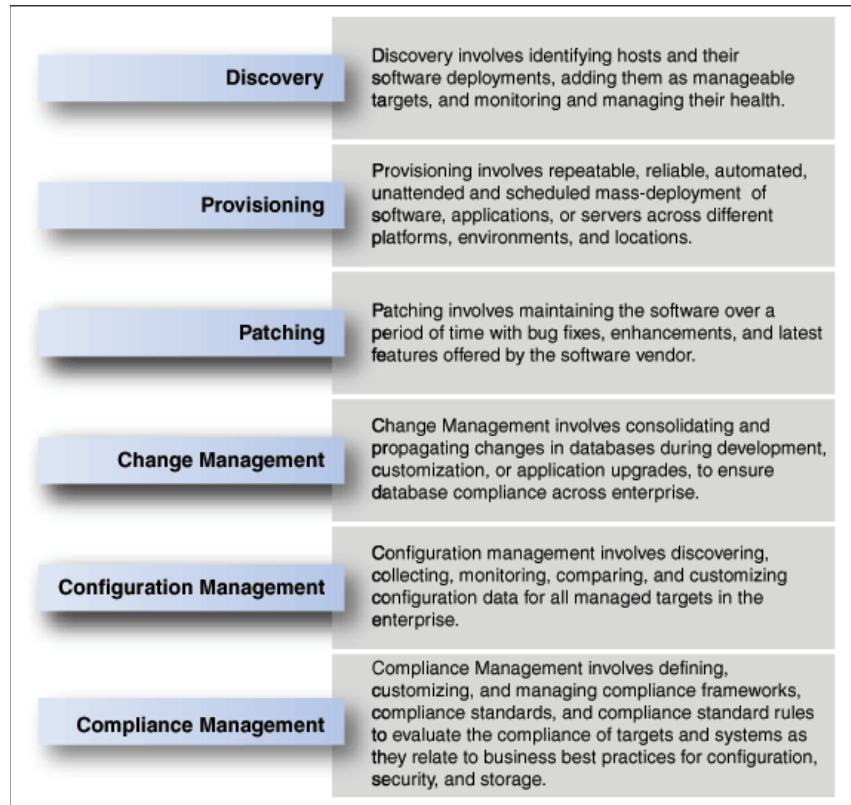


Table 1–1 describes each of these lifecycle management solutions.

Table 1–1 Lifecycle Management Solutions

Solution Area	Coverage
Discovery	<ul style="list-style-type: none"> Automatically discovers software deployments using IP scanning techniques (NMAP). Converts unmanaged software deployments to managed targets in Cloud Control so that their health can be monitored. Offers an integrated workflow for deploying Oracle Management Agents and discovering targets on selected auto-discovered hosts.
Provisioning	<ul style="list-style-type: none"> Discovers bare metal servers and live target servers Provisions Linux operating system on bare metal servers (hypervisors and virtual machines) Associates patching templates with provisioning so that patches can be applied automatically once the operating system is provisioned Provisions of Oracle Databases, Oracle Real Application Clusters (Oracle RAC), Oracle Grid Infrastructure (for standalone servers and clustered environments) Supports initial setup through OneCommand utility and ongoing database provisioning for Exadata Database machines Provisions Oracle Fusion Middleware, Oracle SOA Suite, SOA Artifacts, Oracle BPEL, Oracle Service Bus, Java EE Applications, Oracle Application Server Supports mass upgrade of single instance, Oracle RAC, and Oracle RAC One database instances one at a time

Table 1–1 (Cont.) Lifecycle Management Solutions

Solution Area	Coverage
Patching	<ul style="list-style-type: none"> ■ Offers an integrated patching workflow with My Oracle Support—access to recommendations, search patches, and so on. ■ Orchestrates patching workflow using <i>Patch Plans</i>, including automated selection of deployment procedures and analysis of the patch conflicts. ■ Validates patches for applicability in your environment, validates patch plans, and automatically receives patches to resolve conflicts. ■ Helps you save successfully analyzed or deployable patch plans as patch templates, which contain a predetermined set of patches and deployment options saved from the source patch plan. ■ Offers out-of-place patching (only for standalone databases), in-place patching, and rolling and parallel patching modes, both in offline and online mode.
Change Management	<ul style="list-style-type: none"> ■ Captures database object definitions and initialization parameters at different points in time. ■ Compares a baseline or a database and another baseline or a database. ■ Propagates changes from database definitions and initialization parameters captured in a baseline or from a database to a target database. ■ Specifies, groups, and packages object metadata changes. Create change plans from ad hoc changes, comparison-based differences, or developer tools. ■ Compares data between a local and remote database, and determines how seed data customizations will be affected by application upgrades.
Configuration Management	<ul style="list-style-type: none"> ■ Searches configuration data across the enterprise. ■ Displays configuration data in the context of a single managed entity—configuration item types and properties, system configuration data, system target relationships, custom configuration data. ■ Monitors change activity across the enterprise—includes changes both to configurations and to relationships, which are associations that exist among managed entities. ■ Compare configurations of a particular target type using comparison templates, which enable you to ignore the obvious differences and set alerts on critical issues that need immediate attention. ■ Identifies files and other configuration data that Cloud Control does not already collect from well-known target types or from a target type introduced as part of the custom configuration definition. Offers a set of custom configurations called blueprints, which lay out precisely the files and data to collect for a given platform such as Apache Tomcat. ■ Creates new relationships between managed entities using the Topology Viewer or a generic system target type. Helps you perform dependency analysis and impact analysis on assets in your enterprise using the Topology Viewer.
Compliance Management	<ul style="list-style-type: none"> ■ Evaluates the compliance of targets and systems as they relate to your business best practices for configuration, security, and storage. ■ Advises of how to change configuration to bring your targets and systems into compliance. ■ Helps you define, customize, and manage Compliance frameworks, Compliance standards, Compliance standard rules. ■ Helps you test your environment against the criteria defined for your company or regulatory bodies using these self-defined entities

Note: The provisioning and patch management solutions are essentially based on deployment procedures, which are Oracle-supplied predesigned procedures that help you accomplish the provisioning and patching tasks. Deployment procedures contain a hierarchal sequence of steps, where each step might contain a sequence of other steps. Essentially, they encapsulate the workflow of all the tasks that need to be performed for a provisioning or patching operation. For more information about deployment procedures, see [Chapter 32](#). For information about the default deployment procedure that you must use for your provisioning or patching operation, refer to the respective chapters.

1.2 Information Map

[Table 1–2](#) lists the chapters and sections relevant to the various lifecycle management solutions offered by Cloud Control. Consider this an information roadmap to learn about the solution and perform the required operations.

Table 1–2 Information Map for Lifecycle Management Solutions

Target Name	Solution Area	Reference Links
Database		
Single-Instance Database	Discovery	<ul style="list-style-type: none"> ▪ Discovering Hosts and Targets Automatically ▪ Discovering Hosts and Targets Manually
	Provisioning	<ul style="list-style-type: none"> ▪ Provisioning Oracle Databases ▪ Provisioning Oracle Grid Infrastructure for Oracle Databases ▪ Creating Databases
	Upgrade	Upgrading Databases
	Patching	Patching Software Deployments
	Change Management	Managing Database Configuration Changes
	Configuration Management	Managing Configuration Information
	Compliance Management	Managing Compliance
Oracle Real Application Server (Oracle RAC)	Discovery	<ul style="list-style-type: none"> ▪ Discovering Hosts and Targets Automatically ▪ Discovering Hosts and Targets Manually
	Provisioning	<ul style="list-style-type: none"> ▪ Provisioning Oracle Grid Infrastructure for Oracle Real Application Clusters Databases ▪ Provisioning Oracle Real Application Clusters for 10g and 11g ▪ Extending Oracle Real Application Clusters ▪ Deleting or Scaling Down Oracle Real Application Clusters
	Patching	Patching Software Deployments
	Change Management	Managing Database Configuration Changes
	Configuration Management	Managing Configuration Information

Table 1–2 (Cont.) Information Map for Lifecycle Management Solutions

Target Name	Solution Area	Reference Links
	Compliance Management	Managing Compliance
Oracle RAC One Database	Discovery	<ul style="list-style-type: none"> ■ Discovering Hosts and Targets Automatically ■ Discovering Hosts and Targets Manually
	Provisioning	Provisioning Oracle Real Application Clusters One (Oracle RAC One) Node Databases
	Change Management	Managing Database Configuration Changes
	Configuration Management	Managing Configuration Information
	Compliance Management	Managing Compliance
Oracle Database Replay Client	Discovery	<ul style="list-style-type: none"> ■ Discovering Hosts and Targets Automatically ■ Discovering Hosts and Targets Manually
	Provisioning	Provisioning Oracle Database Replay Client
	Change Management	Managing Database Configuration Changes
	Configuration Management	Managing Configuration Information
	Compliance Management	Managing Compliance
Fusion Middleware		
Oracle Fusion Middleware	Discovery	<ul style="list-style-type: none"> ■ Discovering Hosts and Targets Automatically ■ Discovering Hosts and Targets Manually
	Provisioning	<ul style="list-style-type: none"> ■ Provisioning WebLogic Domains and Middleware Homes ■ Scaling Up / Scaling Out WebLogic Domains
	Configuration Management	Managing Configuration Information
	Compliance Management	Managing Compliance
Java EE Applications	Discovery	<ul style="list-style-type: none"> ■ Discovering Hosts and Targets Automatically ■ Discovering Hosts and Targets Manually
	Provisioning	Deploying / Redeploying / Undeploying Java EE Applications
	Configuration Management	Managing Configuration Information
	Compliance Management	Managing Compliance
Coherence Nodes and Clusters	Discovery	<ul style="list-style-type: none"> ■ Discovering Hosts and Targets Automatically ■ Discovering Hosts and Targets Manually
	Provisioning	Provisioning Coherence Nodes and Clusters
	Configuration Management	Managing Configuration Information
	Compliance Management	Managing Compliance

Table 1–2 (Cont.) Information Map for Lifecycle Management Solutions

Target Name	Solution Area	Reference Links
Oracle SOA Artifacts and Composites	Discovery	<ul style="list-style-type: none"> ■ Discovering Hosts and Targets Automatically ■ Discovering Hosts and Targets Manually
	Provisioning	Provisioning SOA Artifacts and Composites
	Configuration Management	Managing Configuration Information
	Compliance Management	Managing Compliance
Oracle Service Bus	Discovery	<ul style="list-style-type: none"> ■ Discovering Hosts and Targets Automatically ■ Discovering Hosts and Targets Manually
	Provisioning	Provisioning Oracle Service Bus Resources
	Configuration Management	Managing Configuration Information
	Compliance Management	Managing Compliance
Oracle BPEL Process Manager	Discovery	<ul style="list-style-type: none"> ■ Discovering Hosts and Targets Automatically ■ Discovering Hosts and Targets Manually
	Provisioning	Provisioning Oracle BPEL Processes
	Configuration Management	Managing Configuration Information
	Compliance Management	Managing Compliance
Oracle Application Server	Discovery	<ul style="list-style-type: none"> ■ Discovering Hosts and Targets Automatically ■ Discovering Hosts and Targets Manually
	Provisioning	Provisioning Oracle Application Server
	Patching	Patching Software Deployments
	Configuration Management	Managing Configuration Information
	Compliance Management	Managing Compliance
Operating System		
Oracle Linux, Red Hat Enterprise Linux (RHEL), SuSE Linux (SLES)	Discovery	<ul style="list-style-type: none"> ■ Discovering Hosts and Targets Automatically ■ Discovering Hosts and Targets Manually
	Provisioning	Provisioning Bare Metal Servers
	Patching	Patching Linux Hosts
	Configuration Management	Managing Configuration Information
	Compliance Management	Managing Compliance

Setting Up Your Infrastructure

This chapter describes the infrastructure requirements you must meet before you start using the lifecycle management features. This chapter is essentially for administrators or designers who create the infrastructure. The requirements described in this chapter have to be performed just once.

This chapter covers the following:

- [Getting Started](#)
- [Setting Up Oracle Software Library](#)
- [Setting Up Credentials](#)
- [Creating Enterprise Manager User Accounts](#)
- [Setting Up My Oracle Support](#)
- [\(Additional\) Configuring Self-Update](#)
- [\(Additional\) Setting Up E-mail Notifications](#)

2.1 Getting Started

This chapter helps you get started by providing an overview of all the steps involved in setting up your infrastructure. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully set up your infrastructure for carrying out all the lifecycle management tasks, including Patching and Provisioning.

[Figure 2-1](#) is a pictorial representation of the sequence of steps you must perform in order to setup your infrastructure.

Figure 2-1 *Setting Up Your Infrastructure WorkFlow*



Click the reference links provided against the steps in the [Table 2-1](#) for more information on each of the sections.

Table 2–1 Getting Started with Setting Up Your Infrastructure

Step	Description	Reference Links
Step 1	Setting Up Software Library	Section 2.2
Step 2	Setting Up Credentials	Section 2.3
Step 3	Creating Enterprise Manager User Accounts	Section 2.4
Step 4	Setting Up My Oracle Support Credentials	Section 2.5
Step 5	<i>Additional /Value Add setup (optional)</i> Configuring Self-Update	Section 2.6
Step 6	<i>Additional /Value Add setup (optional)</i> Setting Up E-Mail Notifications	Section 2.7

Note: Ensure that the OMS is patched appropriately to the required level. For information about the patches that need to be applied on the Enterprise Manager Cloud Control Management Server (OMS) for using the Provisioning and Patching features, see My Oracle Support note 427577.1.

2.2 Setting Up Oracle Software Library

Oracle Software Library (Software Library) is one of the core features offered by Oracle Enterprise Manager Cloud Control (Cloud Control). Technically, it is a storage location that stores certified software entities such as software patches, virtual appliance images, reference gold images, application software and their associated directive scripts. In addition to storing them, it also enables you to maintain versions, maturity levels, and states of these software entities.

To access the Software Library console page, in Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching** and then, click **Software Library**. On the Software Library home page, as shown in [Figure 2–2](#), there are two types of folders: Oracle-owned folders (marked by a lock symbol) and User-owned folders.

Figure 2–2 Software Library Console

Software Library maintains entities that represent software patches, virtual appliance images, reference gold images, application software and their associated directive scripts. You can pick any of the Oracle-supplied entities, customize them or create a custom one of your own. Once defined, these reusable entities can be referenced from a Deployment Procedure to automate the patching, provisioning or deployment of the associated software.

Page Refreshed Aug 11, 2011 7:07:32 AM PDT

Actions View View Edit... Delete... Find Name Search

Name	Type	Subtype	Revision	Status	Maturity	Owner	Description
Software Library						ORACLE	Root Folder for Software Library entities
Application Server Provisioning Utilities						ORACLE	Entities belonging to AS Provisioning
Bare Metal Provisioning						ORACLE	Bare Metal Provisioning directory
BPEL Provisioning						ORACLE	BPEL Provisioning Entities
Cloud						ORACLE	Cloud
Coherence Node Provisioning						ORACLE	Coherence Node Provisioning Entities
Common Provisioning Utilities						ORACLE	Directives belonging to Common Provisioning (SIDB and RACPRO)
Components						SYSMAN	Components Folder
Directives						SYSMAN	Directives Folder
Images						SYSMAN	Images Folder
Networks						SYSMAN	Networks Folder
Suites						SYSMAN	Suites Folder
CompositeDeploy						ORACLE	CompositeDeploy Entities
CVU Prerequisite-fixup components						ORACLE	CVU Prerequisite-fixup components belonging to DB Provisioning
DB Provisioning						ORACLE	Directives and Components belonging to DB Provisioning
Fusion Middleware Provisioning Utilities						ORACLE	Directives belonging to FMW Provisioning
Java EE Provisioning						ORACLE	Java EE Application Provisioning Entities
MultiOMS						ORACLE	List of Oracle shipped Directives
Oracle VM Server Provisioning						ORACLE	Oracle VM Server Provisioning directory
OSB Provisioning						ORACLE	OSB Provisioning Entities
Patching						ORACLE	Patching directory
Prerequisite-fixup components						ORACLE	Prerequisite-fixup components Components belonging to DB Prov
Soa Provisioning						ORACLE	SOA Provisioning Entities

To start using the Software Library to upload entities or to access entities, the Software Library Storage Locations must be configured. System Administrators are responsible for configuring the Software Library storage locations, following which the Software Library becomes usable.

Cloud Control offers the following types of storage locations:

- **Upload File Locations:** These locations are configured for storing files uploaded by Software Library as part of creating or updating an entity. The Upload File Locations support two storage options:
 - a. OMS Shared File System
 - b. OMS Agent File System
- **Referenced File Locations:** These are locations that allow you to leverage the organization's existing IT infrastructure (like file servers, web servers, or storage systems) for sourcing software binaries and scripts. Such locations allow entities to refer to files without having to upload them explicitly to a Software Library storage. Referenced File Locations support three storage options:
 - a. HTTP Locations
 - b. NFS Locations
 - c. Management Agent Locations

You can configure the storage locations from the Administrator console. To do so, in Cloud Control, from **Setup** menu, select **Provisioning and Patching**, then select **Software Library**. The Software Library Administration Page as shown in Figure 2–3 appears:

Figure 2-3 Software Library Administration

The screenshot shows the 'Software Library: Administration' page. It includes a breadcrumb 'Software Library > Software Library: Administration' and a refresh indicator. The main heading is 'Upload File Locations' with a sub-tab 'Referenced File Locations'. Below this, there is a 'Storage Type' dropdown menu set to 'OMS Shared Filesystem'. A descriptive paragraph explains that these locations must be locally accessible by all OMS instances. Below the text are action buttons: '+ Add...', 'Edit...', and 'Migrate and Remove'. A table lists the configured file locations.

Name	Status	Location	Associated Entities	Total Space	Available Space	Last Refreshed
Testing	Active	/scratch/nbhaktha/swlib/	Show	96.462 GB	61.662 GB	Thu Aug 11 07:11:34 PDT 2011

See Also: For information on configuring Software Library, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*

2.3 Setting Up Credentials

Credentials are identity information stored in Cloud Control, and are used to access targets that are monitored, and managed by Cloud Control. Cloud Control allows you to save your operating system username/password with a unique name as Named Credentials for normal user (*Oracle*). Alternately, if you have `root` privileges, then the `root` account details can be saved with a unique name as Named Credentials for the privileged users.

Primarily, the two types of credentials available in Cloud Control are:

- Named Credentials:** A Named Credential specifies a users' authentication information on a system. Named credentials can be a username/password pair like the operating system login credentials, or Oracle home owner credentials primarily used for performing operations such as running jobs, patching and other system management tasks.
- Privileged Credentials:** Privileged Credentials specifies root users' authentication information on a system. Privileged credentials are the root account details used to perform privileged actions like executing root scripts. Privileged credentials are intended for privileged or power users. In Enterprise Manager 11g, each provisioning user required `sudo` privileges that had to be explicitly granted. However, in Enterprise Manager 12c, you must set up privileged credentials to perform typical root user actions with `sudo` privileges.

Cloud Control allows you the flexibility of saving the Named Credentials and the Privileged Credentials for future use as **Preferred Credentials**.

The advantages of saving the credentials are:

- You do not have to expose the credential details to all the users.

- It saves your time and effort as you do not have to specify the user name and password every time for each Oracle home or host machine, you can instead select a named profile that will use the saved credentials.

Important: If you do not have the host credentials, for example the *Oracle* user account details, or the *root* credentials to the host machine, then you can use Sudo or PowerBroker utilities provided by the Privilege Delegation framework to switch users, and complete the task. For more information about Configuring Privilege Delegation, see [Section 2.3.3](#).

To perform any of the provisioning and patching tasks in Cloud Control, you need to set up Named Credentials for normal operating system user account (*Oracle*) and Named credentials for privileged user accounts (*root*). If you do not have access to either *Oracle* account or *root* account, then you can use SUDO or PowerBroker access to switch users to perform the tasks, this is called Privilege Delegation. Privilege Delegation is a framework that allows you to use either SUDO or PowerBroker to perform an activity with the privileges of another user (locked accounts).

The following table describes the steps to be performed for setting up credentials:

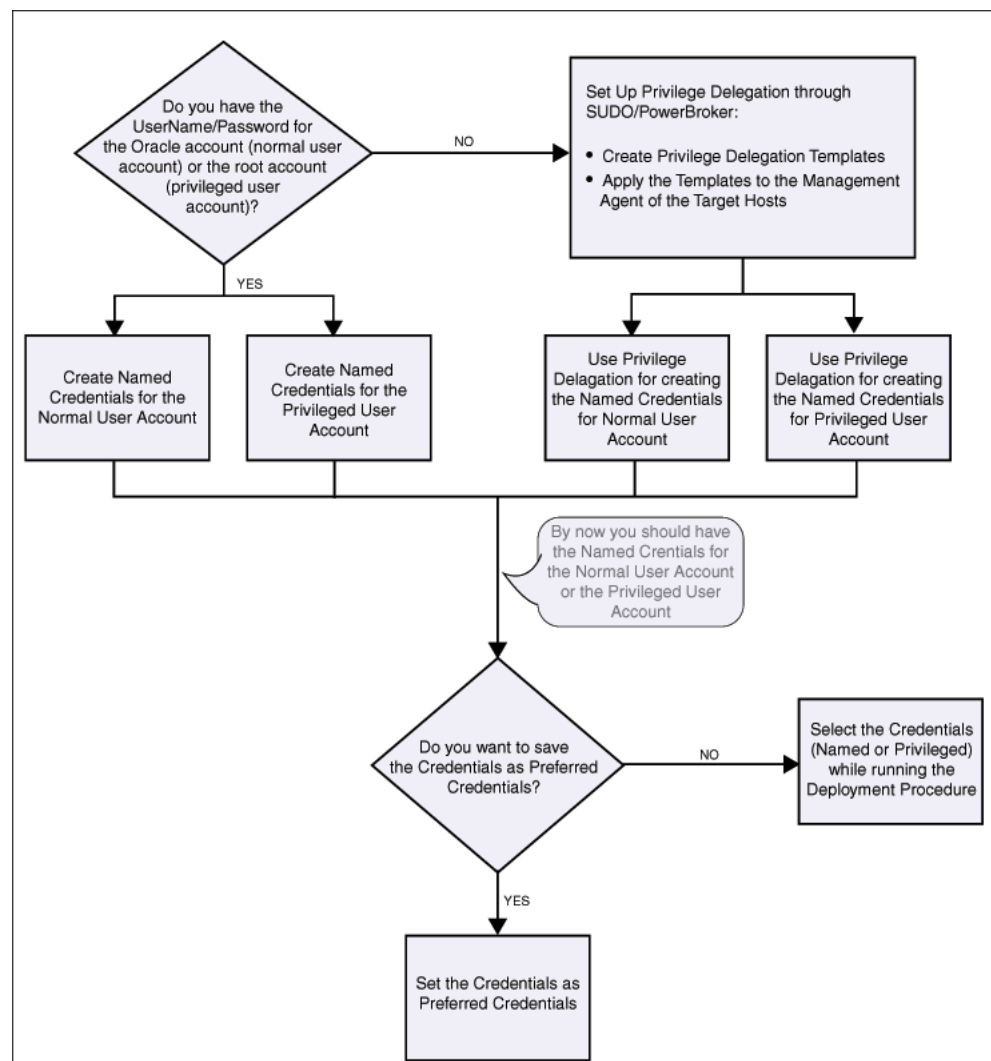


Table 2–2 Setting Up Enterprise Manager Credentials

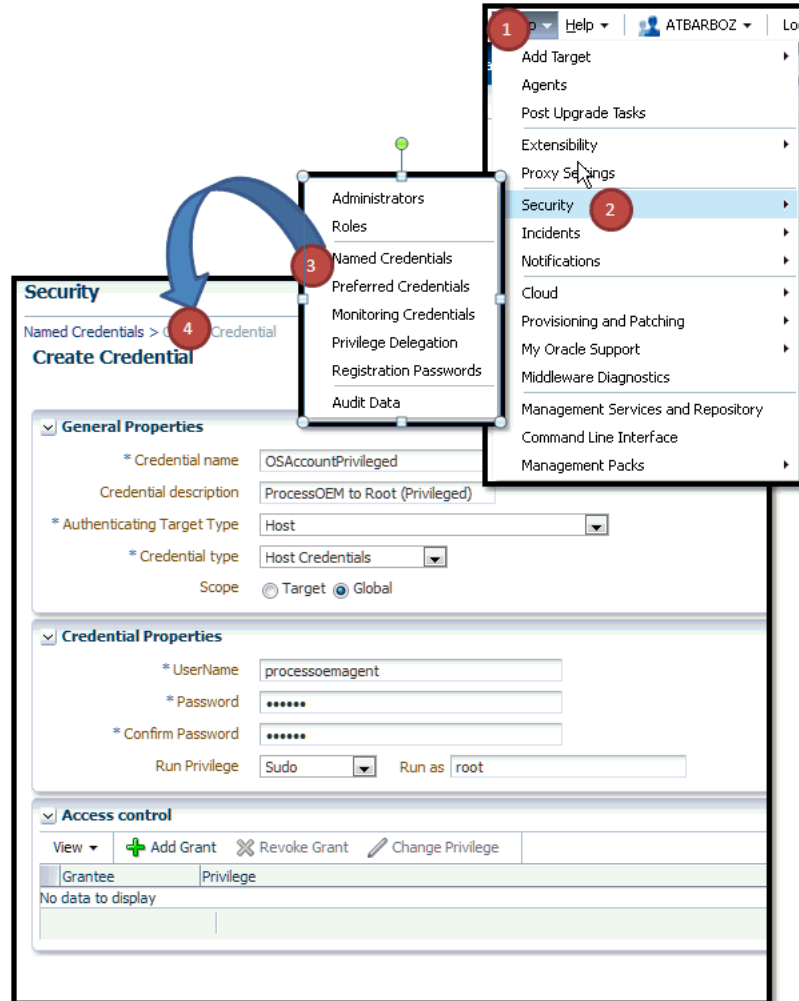
Use Case	Steps to be performed
<p>If you do not have direct access or the required credentials for the normal operating system user account (<i>Oracle</i>)</p> <p>OR</p> <p>If you do not have direct access or the required credentials for the privileged account (<i>root</i>).</p>	<p>Do the following:</p> <ol style="list-style-type: none"> Set up the Privilege Delegation as follows: <ol style="list-style-type: none"> Create Privilege Delegation (PDP) Template either for SUDO or PowerBroker. To do so, see Section 2.3.3.3 Apply the created template on the Management Agents of the target hosts. Create Named Credentials for normal operating system user account(<i>Oracle</i>) with privileges to run as SUDO or PowerBroker, for more information see Section 2.3.1 <p>OR</p> <p>Create Named Credentials for privileged users account (<i>root</i>) with privileges to run as SUDO or PowerBroker, for more information see Section 2.3.2.</p> <ol style="list-style-type: none"> Save the Named credential for normal operating system account or the named credentials for the privileged user account as Preferred Credential. To do so, see Section 2.3.4.
<p>If you have direct access or the required credentials for the normal operating system user account (<i>Oracle</i>)</p> <p>OR</p> <p>If you have direct access or the required credentials for the privileged account (<i>root</i>).</p>	<p>Do the following:</p> <ol style="list-style-type: none"> Create Named Credentials for normal operating system user account (<i>Oracle</i>), for more information see Section 2.3.1. <p>OR</p> <p>Create Named Credentials for privileged user accounts (<i>root</i>) Credentials, for more information see Section 2.3.2.</p> <ol style="list-style-type: none"> Save the Named credential for normal operating system account or the named credentials for the privileged user account as Preferred Credential. To do so, see Section 2.3.4.

2.3.1 Setting Up Named Credentials

To create a named credentials, follow these steps:

- In Cloud Control, from the **Setup** menu, select **Security**, then select **Named Credentials**.
- On the Named Credentials page, click **Create**.
- On the Create Credentials page, in the General Properties section, provide the following details:
 - Enter a unique **Credential Name**, and provide a description.
 - Select **Host** as the Authentication Target Type, and **Host Credentials** as the Credential type
 - Select **Global** to use the same credentials for all the targets.
- On the Create Credentials page, in the Credential Properties section, enter the **UserName** and **Password** required to access the host machine, and from the Run Privilege drop down list, do one of the following:
 - Select **None**, if you are using operating system host credentials (like *Oracle*) or the Oracle Home Owner credentials.

- When you do not have access to the operating system host credentials or the root credentials of the host machine, then select **Sudo** or **PowerBroker** to sudo (or pbrun) to the host machine using the credentials of another operating system user. To use the credentials of other users, in the **Run As** field, you need to enter operating system host credentials (like *Oracle*) or Oracle Home owner credentials of the host user.



- On the Create Credentials page, in the Access Control section, click **Add Grant** to grant privileges on the named profile to the selected Administrators or roles. By default the selected Administrator is granted View privilege.

Note: To enable Administrators (or users) to access, and leverage an OMS Agent Filesystem Software Library Location, the owner of the Named Credential must ensure that an explicit View privilege is granted to all the Administrators accessing the OMS Agent location. To do so, you can either click **Add Grant** and add the names of the administrators while creating the Named Credential as mentioned in this section, or edit an existing Named Credential to grant privileges to other Administrators (or users) by following these steps:

1. In Cloud Control, from the **Setup** menu, select **Security**, then select **Named Credentials**.
2. On the Named Credentials page, click **Manage Access**.
3. On the Manage Access page, click **Add Grant** to add a user, or **Change Privilege** to edit the privileges of an existing user.
4. Click **Save**.

For example, if you have a Cloud Plug-in installed, and are using the Cloud features in Enterprise Manager, then ensure that the `CLOUD_ENGINE_USER` is also granted **View** privileges on credentials associated with Software Library. Since the `CLOUD_ENGINE_USER` is a hidden user account, the owner of the named credential will not be able to grant him View privileges from the Enterprise Manager UI. To handle this situation, (especially on a Windows host where OMS Agent Filesystem is the recommended approach for setting up Software Library) you can run the following EMCLI commands:

```
emcli login -username=<username -password =<>
emcli grant_privs -name=CLOUD_ENGINE_USER -privileges="GET_CREDENTIAL;CRED_ANME=<>:CRDED_OWNER=<>
```

To change the privilege, select the administrator, and click **Change Privilege**. In the Select Privilege dialog box, change the privilege to **Edit** or **Full**, and then click **OK**.

6. After entering all the details, click **Test and Save**. If the host credentials are correct, then the test is successful and the credentials get saved.

2.3.2 Setting Up Privileged Credentials

To create a privileged credentials, follow these steps:

1. Create the Named credentials using the steps mentioned in [Section 2.3.1](#).
2. On the Named Credentials page, select the credential, and then click **Edit**.
3. On the Edit Credential Properties page, in the Credential Properties section, edit the existing **UserName** and **Password** required to access the host machine, and from the Run Privilege drop down list, do one of the following:
 - Select **None**, if you are using operating system host credentials (like *Oracle*) or the Oracle Home Owner credentials.
 - When you do not have access to the operating system host credentials or the root credentials of the host machine, then select **Sudo** or **PowerBroker** to `sudo` (or `pbrun`) to the host machine using the credentials of another operating system user. To use the credentials of other users, in the **Run As** field, you need to enter operating system host credentials (like *Oracle*) or Oracle Home owner credentials of the host user.

2.3.3 Configuring Privilege Delegation Settings

Cloud Control allows you to run Deployment Procedures using authentication utilities such as SUDO, PowerBroker, and so on. This support is offered using the Privilege Delegation mechanism available in Cloud Control. Privilege Delegation is a framework that allows you to use either SUDO or PowerBroker to perform an activity with the privileges of another user (locked accounts).

Note: The certified SUDO versions are 1.6.7 to 1.6.9. Also, note that SUDO 1.7.2 and higher versions are also supported. The certified PBRUN versions are 4.0.8 and 5.x. Higher versions of these utilities may continue to work unless some fundamental changes have been introduced to their behavior.

All the Deployment Procedures offered by Cloud Control require administrator privileges to run. While most steps within a Deployment Procedure can be run as a normal user, there are some steps that require special permissions and privileges, and unless you provide the administrator's credentials, you cannot proceed with the deployment.

Note: To run the procedure on a Windows host which involves executing some Software Library entities (for example, directive scripts), you (*the Windows user*) must be granted the following privileges:

- Act as part of the operating system
- Adjust memory quotas for a process
- Logon as batch job
- Replace a process level token

If not, the execution of the directive steps in the procedure may fail.

Under such circumstances, you can do one of the following. Although the former option is recommended, you are always free to use the latter option to suit your needs.

- Customize the Deployment Procedure to disable the steps that require special privileges, run the other steps as a normal user, and have the administrator run the disabled steps later.
- Use authentication utilities to run some steps within the Deployment Procedure with the privileges of another user. The authentication utilities supported by Cloud Control are SUDO and PowerBroker. This support is offered using the Privilege Delegation mechanism available in Cloud Control. For more information, see [Section 2.3.3.3](#).

In particular, this section covers:

- [Using Privilege Delegation](#)
- [Setting up Privilege Delegation](#)
- [Creating Privilege Delegation Templates](#)
- [Testing Privilege Delegation Settings](#)

2.3.3.1 Using Privilege Delegation

While SUDO and PowerBroker are third-party utilities supported in Cloud Control, Privilege Delegation is proprietary to Oracle. Privilege Delegation is a framework that allows you to use either SUDO or PowerBroker to perform an activity with the privileges of another user.

Privilege Delegation can use either SUDO or PowerBroker, but not both, and the settings are only for a single host. Therefore, if a host is set up with `pbrun`, then it will use only `pbrun`.

Privilege Delegation offers the following advantages:

- You have the flexibility to use either SUDO or PowerBroker within the same framework.
- Using the framework, you can now run PowerBroker in a password-less or password-protected mode.
- You can create a template with these Privilege Delegation settings and reuse it for multiple hosts. This not only allows you to standardize Privilege Delegation setting across your enterprise, but also facilitates the process of configuring Privilege Delegation Settings. It simplifies the Privilege Delegation setting management as well.
- You can use the Privilege Delegation settings not only for deployment procedures, but also for jobs in Cloud Control.
- Privilege Delegation can read passwords from both STDIN and TTY.

2.3.3.2 Setting up Privilege Delegation

Using Privilege Delegation you can ensure that the host user has enough privileges to become a root user, and run root scripts for completing any lifecycle management requirements for your enterprise.

Primarily, there are two approaches for delegating privileges:

- [Updating the SUDOERS File or PBRUN Config File](#)
- [Setting Privileges From Oracle Enterprise Manager Cloud Control](#)

Updating the SUDOERS File or PBRUN Config File

You can either use SUDO or Pluggable Authentication Module (PAM) (for example : `pbrun` (PowerBroker), `suexec`, and so on) as an authentication tool to perform activity over an Oracle Home, when the owner of the Oracle home is not known or locked.

This section covers both the approaches:

- [Using SUDO Authentication Utility](#)
- [Using PBRUN \(PowerBroker\) Authentication Utility](#)

Using SUDO Authentication Utility

If you want to use SUDO authentication utility, then before editing a Deployment Procedure, update the `/etc/sudoers` file to allow a normal user to switch to another user who has the privileges to run the Deployment Procedure. Also, if you want to restrict the normal user to have SUDO access only to certain commands, then specify a list of those commands for which SUDO access is required.

Host level setup can be done manually using Privilege Delegation. If a user running a procedure requires SUDO access to `Oracle` user and `Root` user for running the some commands, then you must edit the Sudoers file to add privileges to these commands.

In Enterprise Manager Cloud Control 12c Release 1 (12.1.0.1) [with or without Bundle Patch 1], nmosudo was located in the agent instance directory. For example, /u01/oracle/agent/agent_inst/bin/nmosudo.

In Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2), this location has changed. Now, nmosudo is present in the sbin directory, which is in the agent base directory. For example, /u01/oracle/agent/sbin/nmosudo.

Therefore, when you install or upgrade to Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2), you must modify the PDP configuration files to update the new location of nmosudo.

For example, if you use SUDO as your PDP, the configuration file for sudo is typically /etc/sudoers. In this file, update the following entry with the new location to nmosudo.

```
sudoer ALL : oracle /eminstall/basedir/sbin/nmosudo *
```

#Sample sudoersfile should have following entry#

If you do not have access to oracle and root accounts, then add the following entries into the file:

```
johndoe ALL=(oracle) /u01/oracle/agent/sbin/nmosudo
johndoe ALL=(root) /u01/oracle/agent/sbin/nmosudo
```

If you have access to the oracle account, but not to the root account, then only add the following entry into the file:

```
johndoe ALL=(root) /u01/oracle/agent/sbin/nmosudo
```

Where,

johndoe refers to the user who has been given the SUDO access to Oracle and Root accounts for running the nmsudo command.

Note: To preserve the environment variable details, update privilege delegation settings to include -E parameter. However, to use the -E option in the SUDO command, you must upgrade to the SUDO version 1.7.2 or higher. The following examples describes the usage of -E option:

```
sudo -E -u %RUNAS% %COMMAND%.
```

Using PBRUN (PowerBroker) Authentication Utility

If you want to use PBRUN authentication utility, then before editing a Deployment Procedure, update the /etc/pb.conf file to allow a normal user to switch to another user who has the privileges to run the Deployment Procedure.

For example, a typical PBRUN config file must look like this:

A typical pbrun config file from /etc/pb.conf file config

```
if(user=="johndoe")
if(command=="/usr/oracle/agent/agent12c/agent_inst/bin/nmosud" )
// /usr/oracle/agent/agent12c/ is the Agent Home
{
switch (requestuser
{
case "root":
runuser="root";
break;
case "oracle":
```

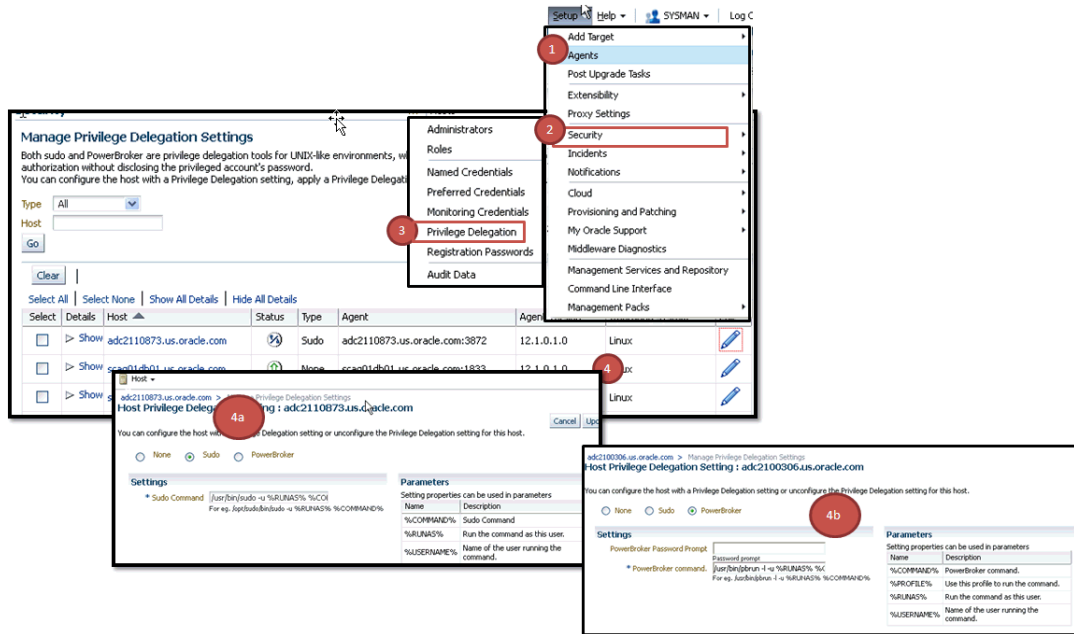
```

        runuser="oracle";
        break;
    default:
        reject;
    }
accept;
}

```

Setting Privileges From Oracle Enterprise Manager Cloud Control

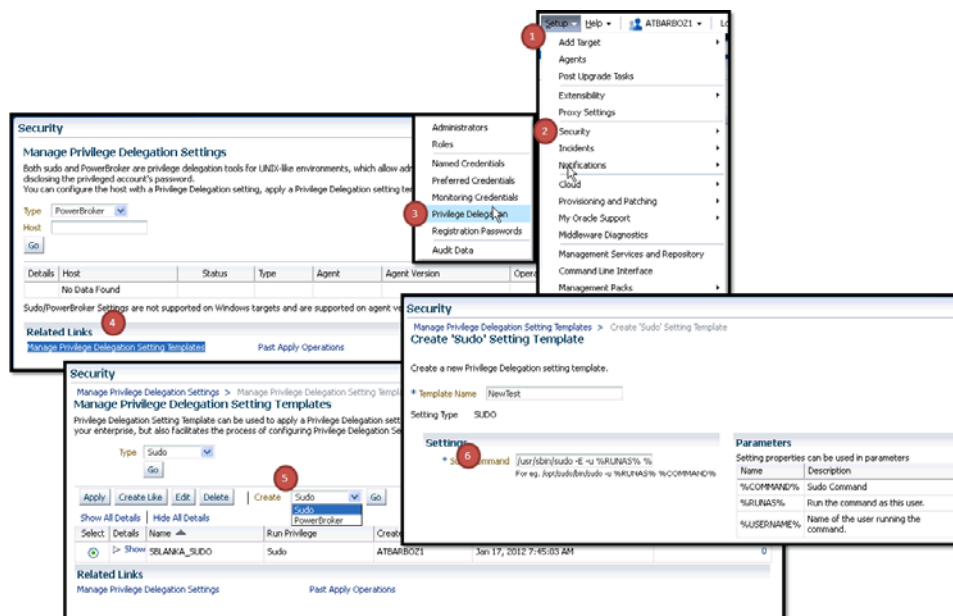
For setting privileges from Cloud Control, follow these steps:



1. In Cloud Control, from the **Setup** menu, select **Security**, then select **Privilege Delegation**.
2. On the Manage Privilege Delegation Setting page, select the host name, and then click **Edit**.
3. On the Host Privilege Delegation Setting: <target name> page, select **Sudo** or **PowerBroker**, and specify the location where SUDO or PowerBroker is located (for PowerBroker, you can optionally provide the password prompt) to configure the host with a Privilege Delegation setting.
4. Click **Update**.

2.3.3.3 Creating Privilege Delegation Templates

If you want to use Privilege Delegation authentication utility, then before editing a Deployment Procedure, create a Privilege Delegation template with the required settings for a host.



To do so, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Security**, then select **Privilege Delegation**.
2. On the Manage Privilege Delegation Settings page, from the Related Links section, click **Manage Privilege Delegation Settings Template**.
3. On the Manage Privilege Delegation Settings Templates page, from the **Create** list, select a privilege delegation type, either **Sudo** or **PowerBroker**, and click **Go**.
4. On the Create '<delegation type>' Setting Template page, provide a name for the template and specify the location where SUDO or PowerBroker is located (for PowerBroker, you can optionally provide the password prompt), and click **Save**.

For example, if you select **SUDO**, and if sudo is located in the `/usr/sbin/directory`, then in the Sudo Command field you need to enter `/usr/sbin/sudo -E -u %RUNAS% %COMMAND%`.

5. On the Manage Privilege Delegation Setting page, select the template you created and click **Go**.
6. On the Apply '<delegation type>' Setting: New page, click **Add Targets** to apply the privilege delegation template settings to selected hosts, and click **Apply**.

Note: If you do not apply the privilege delegation template to a target, and if you configure a step in the deployment procedure to run in Privilege Delegation mode, then the deployment procedure for that target runs the step in normal mode instead.

2.3.3.4 Testing Privilege Delegation Settings

After creating a privilege delegation template and before applying it to a Deployment Procedure, Oracle recommends you to test the privilege delegation setting.

The following is an example that describes how you can register your credentials as preferred credentials, and also choose to run as another user, and then test the settings

by creating a job that checks whether a command is being as normal user or as another user using privilege delegation mechanism.

1. In Cloud Control, from the **Setup** menu, select **Security**, then select **Privilege Delegation**.
2. On the Manage Privilege Delegation Settings page, from the Related Links section, click **Preferred Credentials**.
3. On the Host Preferred Credentials page, in the Target Preferred Credentials section, select the host, and then click **Set**.
4. In the Select Named Credential dialog box, specify the normal user name, the normal password, and the Run as user name that you want to switch over to using the privilege delegation mechanism. Then click **Test and Save**.
5. After registering the credentials as preferred credentials, from the Enterprise menu, select **Jobs**, and then click **Job Activity**.
6. On the Job Activity page, from the Create Job list, select **OS Command**, and click **Go**.
7. On the Create OS Command Job page, in the General tab, specify a name for the job. Then, from the Target section, click **Add** to add the host on which you want to run the OS command.
8. In the Parameters tab, for **Command**, specify the command id.
9. Click **Submit**.
10. On the Job Activity page, click the job name you just created. Cloud Control displays the status of the job. Click the status column to view its results.

Ideally, Cloud Control should have switched over from normal user to another user, which you specified for **Run as** on the Host Preferred Credentials page, and then run the OS command.

2.3.4 Saving Preferred Credentials

Cloud Control allows you the flexibility of saving the Named and the Privileged Credentials for future use as **Preferred Credentials**.

This section includes:

- [Saving Preferred Credentials for Hosts and Oracle Homes](#)
- [Saving Preferred Credentials to Access My Oracle Support](#)

2.3.4.1 Saving Preferred Credentials for Hosts and Oracle Homes

To save the credentials as preferred credentials in Cloud Control, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Security**, then select **Preferred Credentials**.
2. On the Security page, in the Preferred Credentials section, from the table, select either **Host** or **Oracle Home**, and click **Manage Preferred Credentials**.

Note: For setting up preferred credentials for virtual server targets, select Oracle VM Server as the target type and click the Set Credentials.

- a. If you select **Host** for provisioning tasks, then the Host Preferred Credentials page appears.
- b. On the Host Preferred Credentials page, in the Target Preferred Credentials section, select the host target on which you want to provision, and click **Set**.

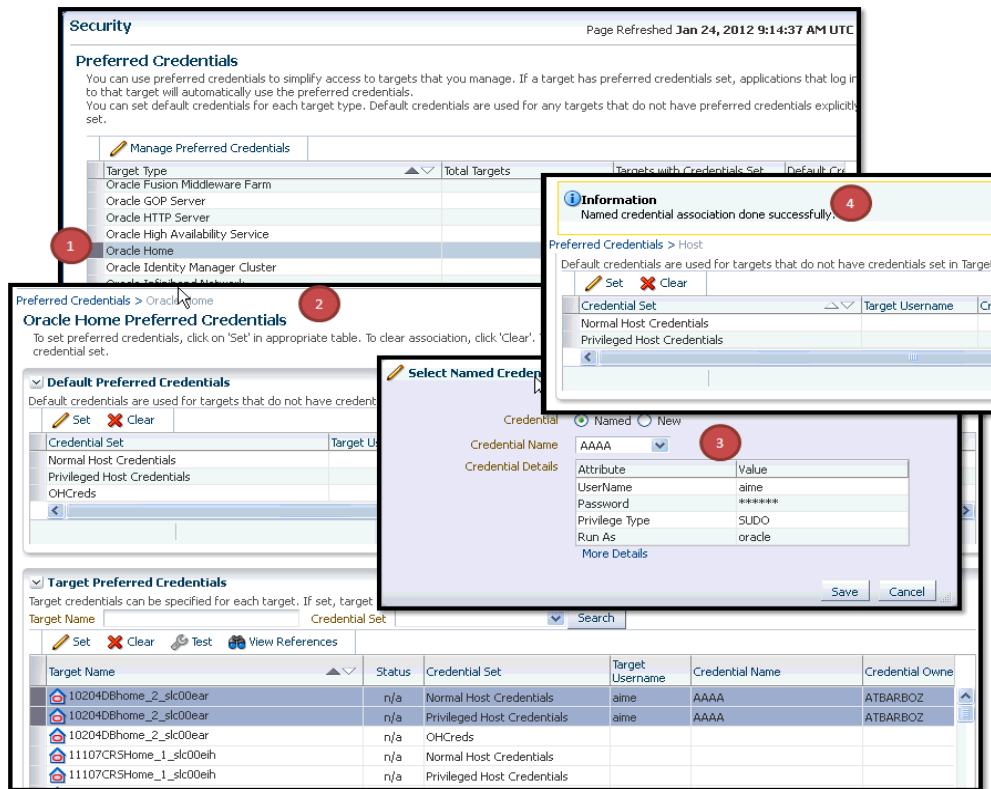
The screenshot displays the Oracle Security console interface. The main content area is titled 'Host Preferred Credentials' and includes a 'Target Preferred Credentials' section with a table of target credentials. A 'Select Named Credential' dialog box is open, allowing the user to configure a new credential. The dialog shows the 'Credential Name' as 'AAAA' and the 'Credential Details' as follows:

Attribute	Value
UserName	aime
Password	*****
Privilege Type	SUDO
Run As	oracle

Below the dialog, a table lists the target credentials:

Target Name	Status	Credential Set	Target Username	Credential Name	Credential Owner
ADC2101857.us.oracle.com	↑	Normal Host Credentials			
ADC2101857.us.oracle.com	↑	Privileged Host Credentials	aime	AAAA	ATBARBOZ
adc2100306.us.oracle.com	↑	Normal Host Credentials	aime	AAAA	ATBARBOZ
adc2100306.us.oracle.com	↑	Privileged Host Credentials			
adc2100914.us.oracle.com	↑	Normal Host Credentials			
adc2100914.us.oracle.com	↑	Privileged Host Credentials			

3. On the Security page, in the Preferred Credentials section, from the table, select either **Host** or **Oracle Home**, and click **Manage Preferred Credentials**
 - a. If you select **Oracle Home** for patching tasks, then the Oracle Home Preferred Credentials page appears.
 - b. On the Oracle Home Preferred Credentials page, in the Target Preferred Credentials section, select the Oracle home you want to patch. Ensure that you set both Normal and Privileged credentials for the targets selected, and click **Set**.



2.3.4.2 Saving Preferred Credentials to Access My Oracle Support

To register the My Oracle Support credentials as preferred credentials in Cloud Control, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **My Oracle Support**, and then, click **Set Credentials**.
2. On the My Oracle Support page, provide the My Oracle Support credentials, and click **Apply**.

Oracle recommends you to register the *My Oracle Support* credentials as preferred credentials in Cloud Control so that you do not have to explicitly provide the credentials every time you access the *My Oracle Support* console, which is integrated within the Cloud Control console.

Note: If you do not have access to My Oracle Support, then you can choose to patch your targets in the offline mode. To enable the offline mode, see [Section 24.2.4.1](#).

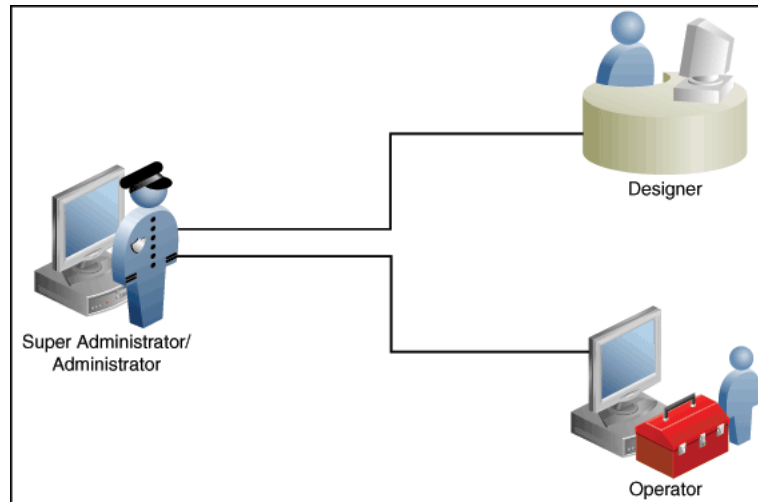
2.4 Creating Enterprise Manager User Accounts

This section describes the following:

- [Overview of User Accounts](#)
- [Creating Designer User Account](#)
- [Creating Operator User Account](#)

2.4.1 Overview of User Accounts

From the Cloud Control, you can create and manage new Enterprise Manager Administrator accounts. Each administrator account includes its own login credentials, as well as a set of roles and privileges that are assigned to the account.



Based on the accesses, the users can be classified as follows:

- Super Administrator
- Designers (EM_ALL_DESIGNER)
- Operators (EM_ALL_OPERATOR)

Super Administrators

Super Administrators are powerful Cloud Control administrators with full access privileges on all targets. They are responsible for creating and administering accounts within the Cloud Control environment. For example, Super Administrators create the Designer and Operator roles, and grant these roles to different users and groups within their enterprise.

Designers

Designers are lead administrators with increased privileges on Deployment Procedures and Software Library. Starting with Cloud Control, designers can create deployment procedure templates using the **Lock down** feature, and save these templates to enforce standardization and consistency. Operator privileges are granted on these templates so that administrators who login as Operators can launch these templates, and run the Deployment Procedure successfully. Doing this ensures that the procedures are less error prone, and more consistent.

For more information about saving deployment procedures using lock downs, see [Section 32.4.2.1](#)

Designers are responsible for performing all the design-time activities like:

- Creating the provisioning profiles in the Software Library.
- Creating components, directives, and images, and storing them in Oracle Software Library.
- Customizing the default deployment procedures according to the needs of the organization.

- Creating patch plans and patch templates.

The predefined Oracle role for a Designer is `EM_ALL_DESIGNER`, this role in turn includes fine grained roles where you can specifically set `EM_PROVISIONING_DESIGNER` for provisioning tasks, and `EM_PATCH_DESIGNER` for patching tasks. For more information about privilege grants to Designers, see [Section 32.2](#).

Operators

Operators are administrators who have restricted privileges on a Deployment Procedure and Software Library. Normally, operators can view and submit a deployment procedure. The Designer user may also grant the Operator the necessary privileges on any targets or entities.

Operators use the infrastructure created by designers and perform run-time activities like:

- Accessing the provisioning profiles present in the Software Library for provisioning procedures.
- Launching software deployments to provision software on selected targets.
- Patching software deployments using patch plans and patch templates.

The predefined Oracle role for an Operator is `EM_ALL_OPERATOR`, this role in turn includes fine grained roles where you can specifically set `EM_PROVISIONING_OPERATOR` for provisioning tasks, and `EM_PATCH_OPERATOR` for patching tasks. For more information about privilege grants to Operators, see [Section 32.2](#).

Note: Designers can choose to perform both design-time and run-time activities, but operators can perform only run-time activities.

2.4.2 Creating Designer User Account

To create a *Designer* user account, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Security**, then select **Administrators**.
2. On the Administrators page, click **Create**.
3. In the Create Administrator wizard, do the following:
 - a. On the Properties page, specify the name *Designer* and provide a password. Leave the other fields blank, and click **Next**.
 - b. On the Roles page, select `EM_ALL_DESIGNER`, and click **Next**.

Note: You can alternately restrict the Designer access to either Provisioning or Patching domains. For granting privileges explicitly for Provisioning, select the `EM_PROVISION_DESIGNER` role. Similarly, for granting designer privileges explicitly for Patching, select the `EM_PATCH_DESIGNER` role.

- c. On the Target Privileges page, select the targets privileges that must be granted to a Designer user account. For information about the target privileges available to an Administrator with Designer role, see [Section 32.2.1](#)
- d. On the Resource Privileges page, select the privileges to be explicitly granted for each of the resource types.

- e. On the Review page, review the information you have provided for this user account, and click **Finish**.

2.4.3 Creating Operator User Account

To create an *Operator* user account, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Security**, then select **Administrators**.
2. On the Administrators page, click **Create**.
3. In the Create Administrator wizard, do the following:
 - a. On the Properties page, specify the name *Operator* and provide a password. Leave the other fields blank and click **Next**.
 - b. On the Roles page, select **EM_ALL_OPERATOR**, and click **Next**.

Note: You can alternately restrict the Operator access to either Provisioning or Patching domains. For granting privileges explicitly for Provisioning, select the `EM_PROVISION_OPERATOR` role. Similarly, for granting designer privileges explicitly for Patching, select the `EM_PATCH_OPERATOR` role.

- c. On the Target Privileges page, select the targets privileges that must be granted to an Operator user account. For information about the target privileges available to an Administrator with Operator role, see [Section 32.2.1](#)
- d. On the Resource Privileges page, select the privileges to be explicitly granted for each of the resource types.
- e. On the Review page, review the information you have provided for this user account, and click **Finish**.

2.5 Setting Up My Oracle Support

For Cloud Control to connect to My Oracle Support for Agent Patching, patching other targets, MOS related tasks, and for Self-Update tasks, you must ensure that you set the proxy server settings and register the details. To do so, follow the instructions outlined in [Section 24.2.3.2](#).

2.6 (Additional) Configuring Self-Update

The Self Update feature enables you to obtain information about updates to Cloud Control components. The Self Update home page can be used to obtain information about new updates and provides a common workflow to review, download and apply the updates. The Self Update console automatically informs you whenever new updates that are applicable to your installation are made available by Oracle.

Software Library components and directives that you can use for provisioning and patching are called provisioning entities. A Provisioning bundle refers to a specific provisioning or patching area, such as database provisioning or FMW provisioning through which Cloud Control delivers updates to customers.

Note: Ensure that the user has `VIEW_ANY_SELFUPDATE` privileges

For applying Oracle-supplied updates to provisioning entities, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Extensibility**, then select **Self Update**.
2. Schedule to download provisioning bundle. The Self-update framework downloads the bundle to a well-defined location. For more information about Self-Update, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
3. From the **Actions** menu, select **Subscribe** to ensure that you receive notification whenever a provisioning bundle is available for download.
4. In the Updates Home page, select update of Type **Provisioning Bundle** and from the **Actions** menu, select **Open**.
5. Apply the provisioning bundle updates manually. Follow instructions as per selected provisioning bundle to apply the update manually.
6. In the Updates Home page, verify that the update is applied.

2.7 (Additional) Setting Up E-mail Notifications

Cloud Control can send e-mail notification every time you run a Deployment Procedure. However, by default, Deployment Procedures do not have this feature enabled. To configure them to send e-mail notifications, you must customize the Deployment Procedure.

For information on how you can customize Deployment Procedures and set up e-mail notifications, see [Chapter 33](#).

Part II

Discovery

This part contains the following chapter:

- [Chapter 3, "Discovering Software Deployments"](#)

Discovering Software Deployments

Discovery is the first step toward monitoring and managing the health of your software deployments. Discovery refers to the process of identifying unmanaged hosts and their software deployments, and adding them as manageable targets in Oracle Enterprise Manager Cloud Control (Cloud Control).

This chapter describes how you can discover the hosts and their software deployments, and add them to Cloud Control. In particular, this chapter describes the following:

- [Discovering Hosts and Targets Automatically](#)
- [Discovering Hosts and Targets Manually](#)

3.1 Discovering Hosts and Targets Automatically

Automatic discovery refers to the process of scanning hosts for Oracle software that can be managed and monitored by Cloud Control. By default, the automatic discovery runs every 24 hours to discover targets.

In automatic discovery, you enable a Management Agent running on the host to run an Enterprise Manager job that scans for unmanaged hosts. You then convert these unmanaged hosts to managed hosts by deploying Management Agents on these hosts, then you search for targets on these managed hosts, and finally you promote these targets to managed target status.

You can configure automatic discovery to set up a schedule for discovery, the target types to be discovered, and the hosts to scan for targets. Discovered hosts can then be promoted to managed target status, enabling Cloud Control to manage and monitor these targets. When new targets are added to your infrastructure, they can be found and brought under management on a regularly-scheduled basis.

Once automatic discovery has been configured, you can check the Auto Discovery Results page on a regular basis to see what targets have been discovered.

For information on automatically discovering and monitoring targets, refer to the chapter *Discovering and Monitoring Targets* in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

3.2 Discovering Hosts and Targets Manually

In addition to automatic discovery, Cloud Control enables you to manually add hosts as well as a wide variety of Oracle software and components as managed targets. When you add a target manually, you do not need to go through the process of discovery by adding the target directly. Discovering targets in this way eliminates the

need to consume resources on the Oracle Management Agent to perform discovery when it is not needed.

For information on manually discovering and monitoring targets, refer to the chapter *Discovering and Monitoring Targets* in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Part III

Database Provisioning

This part contains the following chapters:

- [Chapter 4, "Overview of Database Provisioning"](#)
- [Chapter 5, "Provisioning Oracle Databases"](#)
- [Chapter 6, "Provisioning Oracle Grid Infrastructure for Oracle Databases"](#)
- [Chapter 7, "Provisioning Oracle Grid Infrastructure for Oracle Real Application Clusters Databases"](#)
- [Chapter 8, "Provisioning Oracle Real Application Clusters One \(Oracle RAC One\) Node Databases"](#)
- [Chapter 9, "Provisioning Oracle Real Application Clusters for 10g and 11g"](#)
- [Chapter 10, "Extending Oracle Real Application Clusters"](#)
- [Chapter 11, "Deleting or Scaling Down Oracle Real Application Clusters"](#)
- [Chapter 12, "Provisioning Oracle Database Replay Client"](#)
- [Chapter 13, "Creating Databases"](#)

Overview of Database Provisioning

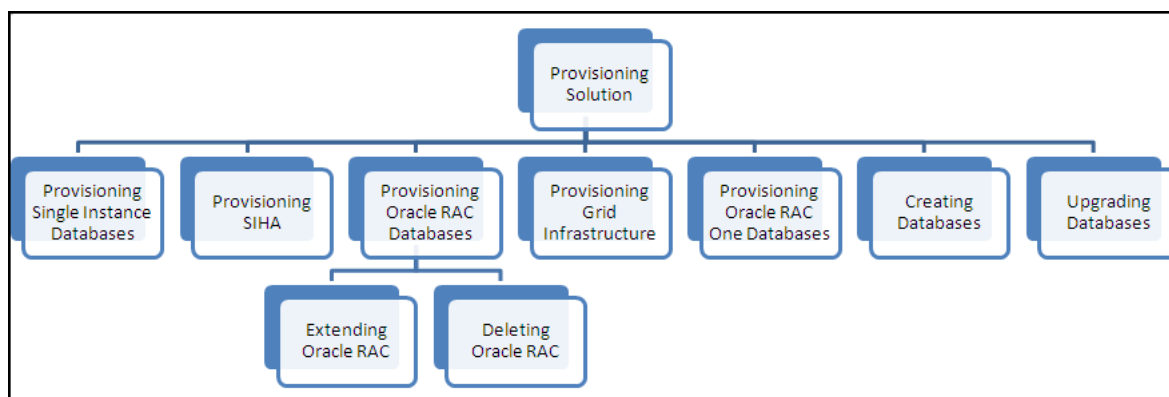
This chapter provides an overview of the database provisioning feature in Oracle Enterprise Manager Cloud Control (Cloud Control), supported targets and deployment procedures offered by Cloud Control, and the infrastructure you need to set up to get started with database provisioning. In particular, this chapter covers the following:

- [Overview of Database Provisioning Feature](#)
- [Supported Targets and Deployment Procedures for Database Provisioning](#)
- [Setting Up Database Provisioning](#)

4.1 Overview of Database Provisioning Feature

The Provisioning solution is an important part of Lifecycle Management solution offered by Cloud Control. As part of the database provisioning solution, Cloud Control enables you to provision Oracle Databases (also known as single-instance databases) and Oracle Real Application Clusters databases, extend or delete Oracle Real Application Clusters nodes, provision Oracle Real Application Clusters One node databases, and also upgrade Oracle single-instance databases in a scalable and automated manner. [Figure 4-1](#) shows the database provisioning solution in Cloud Control.

Figure 4-1 Database Provisioning Solution in Cloud Control



For this release, database provisioning features are as follows:

Designer and Operator Roles

Cloud Control offers clearly-defined administrator roles such as Designers and Operators. With these roles, you also have the capability to lockdown deployment procedure inputs so that operators can deploy standard configurations.

Locking Down Feature in Designer Role

The locking down feature in Database Provisioning enables Designers to lock down the set of variables, such as host targets, credentials, Oracle homes to be provisioned, and others, in the deployment procedure wizard. This enforces standardized deployments and minimizes errors in configurations during mass deployment. The operator can then deploy the procedure that the designer configures and saves in the Procedure Library. For more information about locking down deployment procedures, see [Section 32.4.2.1](#).

Provisioning Profiles and Database Templates

You can create Provisioning Profiles to be used in database provisioning to ensure standardization in deployments and minimize errors. You can also create database templates from the Cloud Control Console to be used in your provisioning activities.

Creating Databases Using Cloud Control

Cloud Control now enables you to create databases from the Cloud Control console. This ensures that you can use a single interface for provisioning and creating databases. For more information about creating databases, see [Chapter 13](#).

Easy to Navigate Database Provisioning Wizards

Designers and Operators can easily use and navigate through the enhanced Database Provisioning wizards in Cloud Control.

Self Update

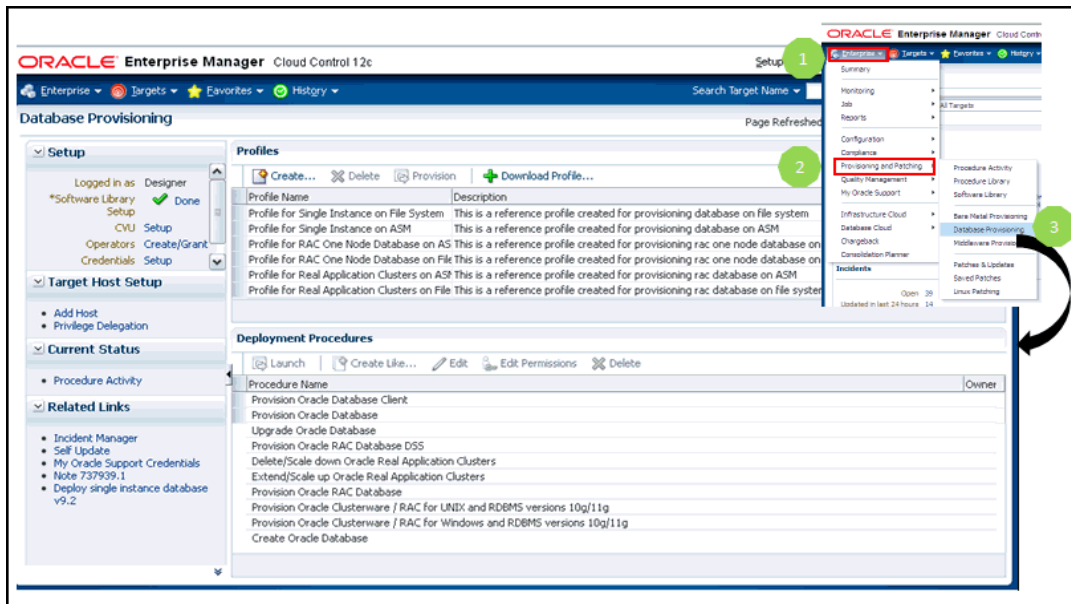
Using the Self Update feature, you can automatically download and install updates to your provisioning entities. For more information on using the Self Update feature to update your provisioning entities, see [Section 2.6](#).

Database Provisioning Console for all Database Provisioning Activities

The Database Provisioning console is a starting point for your database provisioning activities. The console displays information about provisioning setup, profiles, deployment procedures, and information about getting started with provisioning.

[Figure 4–2](#) shows how you can access the Database Provisioning screen from within Cloud Control console.

Figure 4–2 Accessing Database Provisioning Screen



4.2 Supported Targets and Deployment Procedures for Database Provisioning

Cloud Control enables you to perform database provisioning using deployment procedures. A deployment procedure is a set of predefined steps that run one after another to complete the task of provisioning. For information about deployment procedures in general, see [Chapter 32](#).

[Table 4–1](#) lists the database deployment procedures offered by Cloud Control and the various targets that can be provisioned.

Table 4–1 Database Deployment Procedures and Targets Provisioned

Deployment Procedure	Targets Provisioned
Provision Oracle Database	<ul style="list-style-type: none"> ■ Oracle Database (single instance) 10g Release 1 to 11g Release 2 ■ Oracle Grid Infrastructure 11g Release 2 ■ Oracle Automatic Storage Management (Oracle ASM) 11g Release 2
Provision Oracle Real Application Clusters	<ul style="list-style-type: none"> ■ Oracle Real Application Clusters (Oracle RAC) 11g Release 2 ■ Oracle RAC One Node 11g Release 2 ■ Oracle Grid Infrastructure 11g Release 2 ■ Oracle Automatic Storage Management (Oracle ASM) 11g Release 2
Create Oracle Database	<ul style="list-style-type: none"> ■ Oracle Database (single-instance database) 11g Release 2 ■ Oracle Real Application Clusters (Oracle RAC) 11g Release 2 ■ Oracle RAC One Node 11g Release 2

Table 4–1 (Cont.) Database Deployment Procedures and Targets Provisioned

Deployment Procedure	Targets Provisioned
Provision Oracle Clusterware / Oracle RAC for UNIX and RDBMS versions 10g/11g (applicable for UNIX platform)	<ul style="list-style-type: none"> ■ Oracle Real Application Clusters (Oracle RAC) 10g Release 1 to 11g Release 1 ■ Oracle Clusterware 10g Release 1 to 11g Release 1 ■ Oracle Clusterware Automatic Storage Management (Oracle ASM) 10g Release 1 to 11g Release 1
Provision Oracle Clusterware / Oracle RAC for Windows and RDBMS versions 10g/11g (applicable for Windows platform)	<ul style="list-style-type: none"> ■ Oracle Real Application Clusters (Oracle RAC) 10g Release 1 to 11g Release 1 ■ Oracle Clusterware 10g Release 1 to 11g Release 1 ■ Oracle Clusterware Automatic Storage Management (Oracle ASM) 10g Release 1 to 11g Release 1
Extend/Scale Up Oracle Real Application Clusters	Oracle Real Application Clusters (Oracle RAC) 10g Release 1 to 11g Release 2
Delete/Scale Down Oracle Real Application Clusters	Oracle Real Application Clusters (Oracle RAC) 10g Release 1 to 11g Release 2
Provision Oracle Database Client	Oracle Database Client 10g Release 2 to 11g Release 2

Table 4–2 lists various usecases for database provisioning deployment procedures.

Table 4–2 Usecases for Database Deployment Procedures

Deployment Procedure	Usecase	Link
Provision Oracle Database	■ Provisioning and Creating Single-Instance Databases	■ Section 5.3
	■ Provisioning Single-Instance Database with Oracle Automatic Storage Management	■ Section 5.4 ■ Section 5.5 ■ Section 6.2
	■ Provisioning Single-Instance Database Software Only	■ Section 6.3
	■ Provisioning Oracle Grid Infrastructure with Single-Instance Database and Configuring Database with Oracle Automatic Storage Management	
	■ Provisioning Oracle Grid Infrastructure and Single-Instance Database Software Only	
Provision Oracle Real Application Clusters	■ Provisioning Grid Infrastructure with Oracle Real Application Clusters Database and Configuring Database with Oracle Automatic Storage Management	■ Section 7.3 ■ Section 7.4 ■ Section 7.5
	■ Provisioning Oracle Real Application Clusters Database with File System on an Existing Cluster	
	■ Provisioning Oracle Real Application Clusters Database with File System on a New Cluster	

Table 4–2 (Cont.) Usecases for Database Deployment Procedures

Deployment Procedure	Usecase	Link
Create Oracle Database	<ul style="list-style-type: none"> ■ Creating Single-Instance Database ■ Create Oracle Real Application Clusters Database ■ Creating Oracle Real Application Clusters One database 	<ul style="list-style-type: none"> ■ Section 13.2 ■ Section 13.3 ■ Section 13.4
Provision Oracle Clusterware / Oracle RAC for Windows and RDBMS versions 10g/11g	<ul style="list-style-type: none"> ■ Cloning a Running Oracle Real Application Clusters ■ Provisioning Oracle Real Application Clusters Using Gold Image 	<ul style="list-style-type: none"> ■ Section 9.3 ■ Section 9.4 ■ Section 9.5
Provision Oracle Clusterware / Oracle RAC for UNIX and RDBMS versions 10g/11g	<ul style="list-style-type: none"> ■ Provisioning Oracle Real Application Clusters Using Archived Software Binaries 	
Extend/Scale Up Oracle Real Application Clusters	Extending Oracle Real Application Clusters	Section 10.2
Delete/Scale Down Oracle Real Application Clusters	Deleting Oracle Real Application Clusters	Section 11.3 Section 11.4
Provision Oracle Database Client	<ul style="list-style-type: none"> ■ Cloning a Running Oracle Database Replay Client ■ Provisioning Oracle Database Replay Client Using Gold Image ■ Provisioning Oracle Database Replay Client Using Installation Binaries 	<ul style="list-style-type: none"> ■ Section 12.2 ■ Section 12.3 ■ Section 12.4

4.3 Setting Up Database Provisioning

You can provision Oracle Databases, Oracle Real Application Clusters Databases, and Oracle RAC One Node Databases using database templates, installation media, database entities, or use provisioning profiles to standardize deployments.

This section explains the administrator privileges required for provisioning, steps to create provisioning profiles, installation media, and database templates, and also common activities you will need to perform for database provisioning.

- [Meeting Basic Infrastructure and Host Requirements](#)
- [Understanding Administrator Privileges for Provisioning Database](#)
- [Prerequisites for Designers](#)
- [Prerequisites for Operators](#)
- [Creating Provisioning Profiles](#)
- [Creating Installation Media](#)
- [Creating Database Templates](#)
- [Uploading Database Templates to Software Library](#)
- [Creating Database Provisioning Entities](#)
- [Downloading Cluster Verification Utility](#)

Note: If you have upgraded from an older version of Cloud Control to version 12c, you will need to ensure that CSH shell is present as `/bin/csh` before you can run the database provisioning deployment procedures.

4.3.1 Meeting Basic Infrastructure and Host Requirements

Meet the basic infrastructure requirements as described in [Chapter 2](#). Also, ensure that the host is set up for database provisioning entities. Also, ensure that the host is set up for database provisioning entities. For more information about host readiness, see [Appendix B](#).

4.3.2 Understanding Administrator Privileges for Provisioning Database

[Table 4–3](#) describes the roles and the minimum privileges required for using database deployment procedures. These roles are default roles available in Cloud Control. You need not create them, but you must explicitly create administrators based on these roles. For instructions, see [Section 2.4](#).

Table 4–3 Privileges for Using Deployment Procedures

Role	Target Privileges	Resource Privileges	Implementation Recommendation
EM_PROVISIONING_DESIGNER	Operator any target	<ul style="list-style-type: none"> ▪ Resource Type: Deployment Procedure Privilege: Create, Manage Launch Access ▪ Resource Type: Software Library Entity Privilege: Manage Any Software Library Entity 	Required when you want to grant and restrict access to deployment procedures.

Table 4–3 (Cont.) Privileges for Using Deployment Procedures

Role	Target Privileges	Resource Privileges	Implementation Recommendation
EM_PROVISIONING_OPERATOR	<ul style="list-style-type: none"> ▪ Operator any target ▪ Launch DP Permission 	<ul style="list-style-type: none"> ▪ Resource Type: Deployment Procedure Privilege: Create, Manage Launch Access ▪ Resource Type: Software Library Entity Privilege: Manage Any Software Library Entity 	Required when you want to launch deployment procedures.

4.3.3 Prerequisites for Designers

Following are the prerequisites for designers to start database provisioning:

- Ensure that you meet the mandatory infrastructure requirements described in [Chapter 2](#).
- Discover and monitor the destination hosts in Cloud Control. For this purpose, you need the latest version of Oracle Management Agent (Management Agent) on the destination hosts. For more information refer to the Oracle Cloud Control Installation and Basic Configuration Guide. Ensure that the agents are installed in the same location on all hosts.
- Set up the Oracle Software Library (Software Library). Ensure that the installation media, database templates, or provisioning entities are available in the Software Library. For information about creating them, see [Section 4.3](#). Alternatively, use a provisioning profile to store the database template. For information about creating a database provisioning profile, see [Section 4.3.5](#).
- Store the operating system credentials of the destination hosts as preferred credentials in Oracle Management Repository (Management Repository) or use Named Credentials.
If you are using SUDO, PowerBroker, see [Section 2.3.3](#) for information on setting up these authentication utilities.
- Ensure that the operating system groups corresponding to the following roles already exist on the hosts you select for provisioning. If these groups do not exist, then the Deployment Procedure automatically creates them. However, if these have to be created on NIS, then you must create them manually before running the Deployment Procedure. For information about creating these operating system groups, refer to the Oracle Grid Infrastructure Installation Guide 11g Release 2 (11.2).

The Oracle Database user (typically *oracle*) must be a member of the following groups:

- Inventory Group (OINSTALL) as the primary group

- Database Administrator (OSDBA)
- Database Operator (OSOPER)

The Grid Infrastructure user (typically *grid*) must be a member of the following groups:

- Inventory Group (OINSTALL) as the primary group
- ASM Database Administrator (ASMDBA)
- ASM Instance Operator (ASMOPER)
- ASM Instance Administrator (OSASM)
- Ensure that you use an operating system user that has write permission on the following locations:
 - Oracle base directory for Grid Infrastructure where diagnostic data files related to Grid Infrastructure can be stored.
 - Oracle base directory for database where diagnostic data files related to database can be stored.
 - Grid Infrastructure software directory where Grid Infrastructure software can be provisioned.
 - Database software location where database software can be provisioned
 - Working directory where cloning-related files can be staged.
- Ensure that you have `Operator-Any Target` privileges in Cloud Control.
- For provisioning Oracle Real Application Clusters Databases (Oracle RAC), following are additional prerequisites:
 - Meet the hardware, software, and network requirements for Oracle Grid Infrastructure and Oracle RAC installation on the target hosts. For information about the hardware, software, and network requirements for Oracle Grid Infrastructure and Oracle RAC installation, refer to the *Oracle Grid Infrastructure Installation Guide 11g Release 2 (11.2)*.
 - The Oracle RAC Database user must be a member of the group ASM Database Administrator (ASMDBA).

4.3.4 Prerequisites for Operators

Following are the privileges for operators who will run the deployment procedures:

- Ensure that as an operator, you have permissions to view credentials (set and locked by the designer), view targets, submit jobs, and launch deployment procedures.
- Ensure that the operating system groups corresponding to the following roles already exist on the hosts you select for provisioning. The operating system users of these groups automatically get the respective privileges.
 - Inventory Group (OINSTALL)
 - ASM Database Administrator (ASMDBA)
 - ASM Instance Operator (ASMOPER)
 - Database Administrator (OSDBA)
 - Database Operator (OSOPER)
 - ASM Instance Administrator (OSASM)

- Ensure that you have `Operator-Any Target` privileges in Cloud Control.

4.3.5 Creating Provisioning Profiles

Provisioning Profile is an entity which contains software bits and configuration. When a provisioning profile is created from an existing installation, it provides the flexibility to clone either Grid Infrastructure (with software or configuration) and Oracle Database (with software or configuration). You can create database templates using provisioning profiles. A designer or administrator can create a database provisioning profile as a one-time activity; which can be used by operators for mass deployment. Using provisioning profile enables standardization in deployments and reduces need for rescheduling deployments by avoiding errors while configuring deployment procedures.

To create database provisioning profile, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, in the Database System Profile section, click **Create**. The Create Database Provisioning Profile wizard is launched.
3. In the Reference Host page, select the reference host from which you want to create the provisioning profile. Depending on the reference host configuration, you can select to include database gold image, Grid Infrastructure gold image, and their related configuration as part of the provisioning profile.

In the Select Operations to include as part of profile section, select:

- **Oracle Grid Infrastructure Gold Image and its Configuration Properties** to include Grid infrastructure gold image and its configuration in the profile
- **Oracle Database Gold Image** to include Oracle database gold image in the profile
- **Oracle Database Template** to include Oracle database template in the profile

Click **Next**.

4. In the Oracle Home Details page, in the Select Grid Infrastructure section, select the Grid Infrastructure Oracle home from which you want to create the Grid Infrastructure gold image.

In the Select Database Software section, select the database Oracle home from which you want to create the Oracle Database gold image. Specify the temporary **Working Directory** to be used during gold image creation.

Click **Next**.

5. In the Database Details page, select the database from which you want to create the database template. Select **Structure + Data** to include physical and structural files from the database or **Structure Only** to include only the structural files in the template. Select **Convert the file locations to use OFA structure** to ensure that discrepancy in directory structure in the reference host will not affect the database template creation. Click **Next**.

Note: If you have selected **Structure + Data**, then the database target will be shutdown during template creation. You can prevent the database from shutting down, by not selecting the **Blackout the database target during template creation** option.

Note: You can edit and customize the database template you create and then upload the customized template to the Software Library. For information about uploading database templates to Software Library manually, see [Section 4.3.8](#).

6. In the Credentials page, specify the Operating System Credentials for Grid Infrastructure Home, Database Home, and Database. Select Preferred Credentials or Named Credentials. If using Named Credentials, select the credentials or click + to specify new Named Credentials. In the Add Credentials popup, specify the **User Name** and **Password**. Select **Save As** and specify a name for the Credentials, select **Scope** as **Global** if you want to set it for all targets or **Target** if you want to apply it to only the selected target. Select **Set as Preferred Credentials** if you want to set these as the Preferred Credentials. Click **Next**.
7. In the Profile Details page, retain or edit the default details such as **Profile Location** where you want to store the provisioning profile in the Software Library, **Name**, **Description**, **Version**, **Vendor**, **Notes**, and the **Name of Components** included in the profile. The Profile Location will be used to store the gold images and template components created as part of this profile.

In the Software Library Storage section, select the **Software Library Location Type** and **Software Library Location Name**. The **Software Library Storage Location**, **Total Space**, and **Available Space** are displayed. If you have selected Oracle Grid Infrastructure Gold Image Component and Oracle Database Gold Image Component, ensure that 2 GB and 3 GB of space respectively is available.

Click **Next**.

8. In the Review page, ensure that the selections you have made in the previous pages are correctly displayed and click **Submit**. Otherwise, click **Back** repeatedly till you reach the page where you want to make changes. Click **Cancel** to abort the provisioning profile creation. The Deployment Instance Name is generated with the profile name and user name.
9. Once you have submitted the provisioning profile creation job, ensure that the provisioning profile appears in the Database Provisioning page.

4.3.6 Creating Installation Media

To create installation media that can be used for database provisioning, follow these steps:

1. Create a temporary location `mkdir /tmp/installmedia`.
2. Navigate to the following URL:
<http://www.oracle.com/technetwork/database/enterprise-edition/downloads/index.html>
3. Click the See All link for the operating system on which you want to provision the database.
4. Select **Accept License Agreement**.
5. Download zip files 1 and 2 for Database and Grid Infrastructure software to the temporary directory created earlier.
6. Navigate to the temporary directory and extract the contents of the zip files.

For example, to extract the contents of the database software zip files, run these commands:

```
Unzip linux_11gR2_database_1of2.zip
Unzip linux_11gR2_database_2of2.zip
```

7. Create a single zip file with the contents of both the downloaded zip files.

For example, to create a zip for the two database software zip files you downloaded, first extract the contents of each of the zip files as described in the previous step, and then run the following command to create one complete zip file:

```
zip -r linux_11gR2_database.zip database/
```

8. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching** and then select **Software Library**.
9. In Software Library, select the directory where you want to create the installation media component for the database.
10. From the **Actions** menu, select **Create Entity**, then select **Component**.
11. In the Create Entity: Component dialog, select Subtype as **Installation Media** and click **Continue**.
12. In the Create Installation Media: Describe page, enter the Name and Description for the component, and click **Next**.
13. In the Create Installation Media: Configure page, select **Product Version**, **Platform**, and **Product** from the list.

For Product, select **Oracle Database** for Oracle Database, **Oracle Client** for Oracle Database Replay Client, and **Oracle Grid Infrastructure** for Grid Infrastructure software.

Click **Next**.

14. In the Create Installation Media: Select Files page, select **Upload Files**.
 - a. In the Specify destination section, choose a Software Library storage location as the **Upload Location** for the database software.
 - b. In the Specify Source section, select **File Source** as Agent Machine and select the host from which you want to upload the files.
 - c. Click **Add**.
 - d. In the Remote File Browser, click Login As.
 - e. Select the Host Credentials and click **OK**.
 - f. Navigate to the temporary directory and select the zipped database file created earlier.
 - g. Click **Add** and then click **OK**.

Click **Next**.

15. In the Create Installation Media: Review page, review the details you have provided and click **Save and Upload** to save and upload the installation media files to Software Library.

4.3.7 Creating Database Templates

Cloud Control allows you to create database templates that you can use for cloning or creating additional databases. To create database templates, follow these steps:

1. From the **Targets** menu, select **Databases**.
2. In the Databases page, click on the database from which you want to create a template.
3. In the Database home page, from the **Oracle Database** menu, select **Provisioning**, then select **Create Database Template**.
4. In Template Type page, select:
 - **Structure as well as data** to include physical data files and structural information in the template. User-defined schemas and data will be included in the template. Databases created from this type of template will be identical to the source database.
 - **Structure** to include structural information about the source database including tablespace options, initialization parameters, and data files. User-defined schemas and data will not be included in the template.

Select host credentials. You can select **Preferred Credentials**, **Named Credentials**, or **Enter Credentials**.

Click **Next**.

5. In the Template Options page, specify the **Template Name** and **Description**. Specify the template location:
 - Select **Store Template in Software Library** to specify the **Storage Type** and **Location** on the OMS Agent File System or Shared File System.
 - Select **Store Template on the Managed Host** to store template at ORACLE_HOME/assistants/dbca/templates in the target Oracle home.

Specify the database file locations. Select:

- **Use Oracle Flexible Architecture** to convert the location of files in the template to OFA.
- **Maintain File Location** if you want the location of the files in the template to be identical to the source database.

Click **Next**.

6. In the Schedule page, specify the job name and schedule. If you want to run the job immediately, then retain the default selection, that is, **One Time (Immediately)**. If you want to run the job later, then select **One Time (Later)** and provide time zone, start date, and start time details. You can also select to blackout the database during the template creation process. Click **Next**.
7. In the Review page, review the details you have provided for the job and if you are satisfied with the details, then click **Submit Job** to run the job according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes.
8. In the Jobs page, verify that the job has successfully completed and the template has been created as specified.

Note: You can also use Database Configuration Assistant (DBCA) for creating database templates.

You can edit and customize the database template you create and then upload the customized template to the Software Library. For information about uploading database templates to Software Library manually, see [Section 4.3.8](#).

4.3.8 Uploading Database Templates to Software Library

You can edit and customize your database templates and then upload them to Software Library as follows:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library Home page, select the folder where you want to upload the database template.
3. From the **Actions** menu, select **Create Entity**, then select **Component**. Alternately, right click the custom folder, and from the menu, select **Create Entity**, then select **Component**.
4. From the Create Entity: Component dialog box, select **Database Template** and click **Continue**.

Cloud Control displays the Create DatabaseTemplate page.

5. On the Describe page, enter the **Name**, **Description**, and **Other Attributes** that describe the entity.

Note: The component name must be unique to the parent folder that it resides in. Sometime even when you enter a unique name, it may report a conflict, this is because there could be an entity with the same name in the folder that is not visible to you, as you do not have view privilege on it.

Click **+Add** to attach the database template. Select the template as the Source file in the format *templatename.dbt* or *templatename.dbc*. Retain the File Name as displayed. Ensure that the file size is less than 2 MB.

In the **Notes** field, include information related to the entity like changes being made to the entity or modification history that you want to track.

6. On the Select Files page, add all the database template related files.

Select Upload Files to upload all the database template files as follows:

- a. In the Specify Destination section, choose the Software Library location where you want to upload the files.
- b. In the Specify Source section, select the location where you have stored the template files. The location can be your local machine or the agent machine.
- c. Click **+Add** to upload the database template files.

For Structure template, again add the *templatename.dbt* file. In case of Structure And Data template, upload the *templatename.dbc*, *datafiledump.dfb* and the *controlfile.ctl* files. Mark the *templatename.dbc* file as the Main File.

Select Refer Files to refer files from an existing referenced file storage location. Select the Referenced File Location and add the source file.

7. On the Review page, review the details and then click **Save and Upload** to create the component and upload the binary to Software Library.

4.3.9 Creating Database Provisioning Entities

You can create and store provisioning entities in the Software Library to be used for provisioning Oracle databases. Cloud Control allows you to create the following types of database provisioning entities:

- Oracle Database Clone
- Oracle Clusterware Clone

The following subsections explain how to create these provisioning entities:

- [Creating an Oracle Database Clone from a Reference Home](#)
- [Creating an Oracle Database Clone from an External Storage](#)
- [Creating an Oracle Clusterware Clone from a Reference Home](#)
- [Creating an Oracle Clusterware Clone from an External Storage](#)

4.3.9.1 Creating an Oracle Database Clone from a Reference Home

To create an Oracle Database Clone from a reference home, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library Home page, select any custom folder and create the database clone component.
3. From the **Actions** menu, select **Create Entity**, then select **Component**. Alternately, right click the custom folder, and from the menu, select **Create Entity**, then select **Component**.
4. From the Create Entity: Component dialog box, select **Oracle Database Software Clone** and click **Continue**.

Cloud Control displays the Create Oracle Database Software Clone page.

5. On the Describe page, enter the **Name**, **Description**, and **Other Attributes** that describe the entity.

Note: The component name must be unique to the parent folder that it resides in. Sometime even when you enter a unique name, it may report a conflict, this is because there could be an entity with the same name in the folder that is not visible to you, as you do not have view privilege on it.

Click **+Add** to attach files that describe the entity better like readme, collateral, licensing, and so on. Ensure that the file size is less than 2 MB.

In the **Notes** field, include information related to the entity like changes being made to the entity or modification history that you want to track.

6. On the Configure page, from the Create Component from menu, select **Reference Oracle Home** and do the following:
 - a. In the Reference Oracle Home section, click the magnifier icon to select the desired database Oracle home from the list of databases running on the host machine.

The **Oracle Home Location** and **Host Name** fields are populated with the selected values.

- b. In the Oracle Home Credentials section, select the credential type you want to use for accessing the targets you manage. For information about setting credentials, see [Section 2.3](#)
- c. In the Working Directory and Files to Exclude section, enter a **Working Directory** on the host on which you have write permissions, so that the cloned zip file can be created and placed there temporarily.

The **Files to exclude** field is pre-populated with certain types of files or patterns that will be excluded from the cloned zip file. However, you can customize this list based on your requirement.

- d. In the Software Library Upload Location section, select a configured storage location from the list where you want to place the database clone software.

For more information on creating a Software Library Storage Location, see [Section 2.2](#).

7. On the Review page, review the details and then click **Save and Upload** to create the component and upload the binary to Software Library.

4.3.9.2 Creating an Oracle Database Clone from an External Storage

To create an Oracle Database Clone from an external storage, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library Home page, select any custom folder and create the database clone component.
3. From the **Actions** menu, select **Create Entity**, then select **Component**. Alternately, right click the custom folder, and from the menu, select **Create Entity**, then select **Component**.
4. From the Create Entity: Component dialog box, select **Oracle Database Software Clone** and click **Continue**.

Cloud Control displays the Create Oracle Database Software Clone page.

5. On the Describe page, enter the **Name**, **Description**, and **Other Attributes** that describe the entity.

Note: The component name must be unique to the parent folder that it resides in. Sometime even when you enter a unique name, it may report a conflict, this is because there could be an entity with the same name in the folder that is not visible to you, as you do not have view privilege on it.

Click **+Add** to attach files that describe the entity better like readme, collateral, licensing, and so on. Ensure that the file size is less than 2 MB.

In the **Notes** field, include information related to the entity like changes being made to the entity or modification history that you want to track.

6. On the Configure page, from the Create Component from menu, select **Existing Oracle Home Archive** and do the following:
 - a. In the Oracle Home Archive section, select a external storage location from where you can refer to the database clone software. From the **External Storage Location Name** menu, select the location name.

For more information on configuring external storage locations, see [Section 2.2](#).

In **Oracle Home Archive Location**, enter the exact path, which is basically the relative path from the configured location, of the archive file residing on the external storage location. Ensure that the archive file is a valid zip file.

Note: To create the zip file of an Oracle Home, use the following syntax:

```
<ZIP PATH>/zip -r -S -9 -1 <archiveName.zip> <directory or list of files to be archived> -x <patterns to exclude files>
```

- b. In the Oracle Home Properties section, select the **Product, Version, Platform,** and **RAC Home** values, as these configuration properties are particularly useful to search or track an entity.
7. On the Review page, review the details and then click **Save and Upload** to create the component and upload the binary to Software Library.

4.3.9.3 Creating an Oracle Clusterware Clone from a Reference Home

To create an Oracle Clusterware Clone from a reference home, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library Home page, select any custom folder and create the database clone component.
3. From the **Actions** menu, select **Create Entity**, then select **Component**. Alternately, right click the custom folder, and from the menu, select **Create Entity**, then select **Component**.
4. From the Create Entity: Component dialog box, select **Oracle Clusterware Clone** and click **Continue**.

Cloud Control displays the Create Oracle Clusterware Clone : Describe page.

5. On the Describe page, enter the **Name, Description,** and **Other Attributes** that describe the entity.

Note: The component name must be unique to the parent folder that it resides in. Sometime even when you enter a unique name, it may report a conflict, this is because there could be an entity with the same name in the folder that is not visible to you, as you do not have view privilege on it.

Click **+Add** to attach files that describe the entity better like readme, collateral, licensing, and so on. Ensure that the file size is less than 2 MB.

In the **Notes** field, include information related to the entity like changes being made to the entity or modification history that you want to track.

6. On the Configure page, from the Create Component from menu, select **Reference Home** and do the following:
 - a. In the Reference Oracle Home section, click the magnifier icon to select the desired Oracle Clusterware Oracle home from the list of Clusterware homes running on the host machine.

The **Oracle Home Location** and **Host** fields are populated with the selected values.

- b. In the Oracle Home Credentials section, select the credential type you want to use for accessing the targets you manage. For information about setting credentials, see [Section 2.3](#).
- c. In the Working Directory and Files to Exclude section, enter a **Working Directory** on the host on which you have write permissions, so that the cloned zip file can be created and placed there temporarily.

The **Files to exclude** field is pre-populated with certain types of files or patterns that will be excluded from the cloned zip file. However, you can customize this list based on your requirement.

- d. In the Software Library Upload Location section, select a configured storage location from the list where you want to place the Oracle Clusterware clone software.

For more information on creating a Software Library Storage Location, see [Section 2.2](#).

7. On the Review page, review the details and then click **Save and Upload** to create the component and upload the binary to the Software Library.

4.3.9.4 Creating an Oracle Clusterware Clone from an External Storage

To create an Oracle Clusterware Clone from an external storage location, perform the following steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library Home page, select any custom folder and create the database clone component.
3. From the **Actions** menu, select **Create Entity**, then select **Component**. Alternately, right click the custom folder, and from the menu, select **Create Entity**, then select **Component**.
4. From the Create Entity: Component dialog box, select **Oracle Clusterware Clone** and click **Continue**.

Cloud Control displays the Create Oracle Clusterware Clone : Describe page.

5. On the Describe page, enter the **Name**, **Description**, and **Other Attributes** that describe the entity.

Note: The component name must be unique to the parent folder that it resides in. Sometime even when you enter a unique name, it may report a conflict, this is because there could be an entity with the same name in the folder that is not visible to you, as you do not have view privilege on it.

Click **+Add** to attach files that describe the entity better like readme, collateral, licensing, and so on. Ensure that the file size is less than 2 MB.

In the **Notes** field, include information related to the entity like changes being made to the entity or modification history that you want to track.

6. On the Configure page, from the Create Component from menu, select **Existing Oracle Home Archive** and do the following:

- a. In the Oracle Home Archive section, select an external storage location from where you can refer to the Oracle Clusterware clone software. From the **External Storage Location Name** menu, select the location name.

For more information on configuring external storage locations, see [Section 2.2](#).

In **Oracle Home Archive Location**, enter the exact path, which is basically the relative path from the configured location, to the archive file residing on the external storage location. Ensure that the archive file is a valid zip file.

Note: To create the zip file of an Oracle Home, use the following syntax:

```
<ZIP PATH>/zip -r -S -9 -1 <archiveName.zip> <directory or list  
of files to be archived> -x <patterns to exclude files>
```

- b. In the Oracle Home Properties section, select the **Product**, **Version**, and **Platform** values, as these configuration properties are particularly useful to search or track an entity.
7. On the Review page, review the details and then click **Save and Upload** to create the component and upload the binary to Software Library.

4.3.10 Downloading Cluster Verification Utility

Cluster Verification Utility (CVU) performs system checks in preparation for installation, patch updates, or other system changes. You can synchronize cluster verification utility (CVU) binaries with Software Library.

Enterprise Manager, by default, provides a routine job that is scheduled daily to download binaries from My Oracle Support if corresponding binaries in the Software Library need to be updated. If your Enterprise Manager deployment is behind a firewall or a DMZ such that HTTP connection to My Oracle Support is disabled, the routine job will skip its execution. In this case, you can manually download the CVU binaries corresponding to your platform from OTN or My Oracle Support using patch 9288873 as source. You can then synchronize these manually downloaded Cluster Verification Utility (CVU) binaries to Software Library as follows:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Provisioning page, click **CVU Setup**.
3. In the Download Cluster Verification Utility page, select one of the following:
 - a. **Local Machine** to select the CVU binaries from your local computer.
 - b. **Agent Machine** to select the CVU binaries from the agent machine.
4. Click **OK**. This will update the Software Library with the latest cluster verification utility binaries.

Provisioning Oracle Databases

This chapter explains how you can mass-deploy Oracle Databases (also called as single-instance databases) in an unattended, repeatable, and reliable manner, using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Getting Started](#)
- [Oracle Database Topology](#)
- [Provisioning and Creating Oracle Databases](#)
- [Provisioning Oracle Databases with Oracle Automatic Storage Management](#)
- [Provisioning Oracle Database Software Only](#)

5.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in provisioning Oracle Databases. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision single-instance databases. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 5–1 *Getting Started with Provisioning Oracle Databases*

Step	Description	Reference Links
Step 1	<p>Understanding Oracle Database Topology</p> <p>Understand the Database Provisioning feature that is offered by Cloud Control for provisioning single-instance databases.</p>	To learn about Oracle Database topology, see Section 5.2 .
Step 2	<p>Selecting the Use Case</p> <p>This chapter covers a few use cases for provisioning Oracle Database. Select the use case that best matches your requirement.</p>	<ul style="list-style-type: none"> ■ To learn about provisioning and configuring Oracle Database, see Section 5.3. ■ To learn about provisioning Oracle Database with Automatic Storage Management, see Section 5.4. ■ To learn about provisioning Oracle Database software, see Section 5.5.

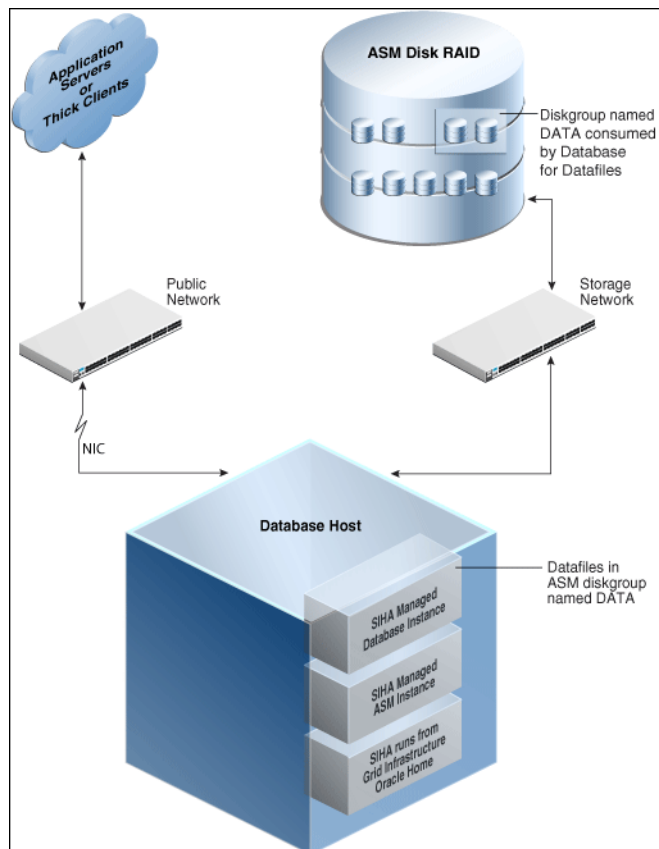
Table 5–1 (Cont.) Getting Started with Provisioning Oracle Databases

Step	Description	Reference Links
Step 3	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	<ul style="list-style-type: none"> ■ To learn about the prerequisites in provisioning and configuring Oracle Database, see Section 5.3.1. ■ To learn about the prerequisites in provisioning Oracle Database with Automatic Storage Management, see Section 5.4.1. ■ To learn about the prerequisites in provisioning Oracle Database software, see Section 5.5.1.
Step 4	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully provision Oracle Database.</p>	<ul style="list-style-type: none"> ■ To provision and configure Oracle Database, see Section 5.3.2. ■ To provision Oracle Database with Automatic Storage Management, see Section 5.4.2. ■ To provision Oracle Database software, see Section 5.5.2.

5.2 Oracle Database Topology

Figure 5–1 shows a typical Oracle Database (single-instance database) topology that you can provision using Cloud Control.

Figure 5–1 Oracle Database Topology



The topology shows a 11.2.0.3 RDBMS managed by Single-Instance High Availability (SIHA) component of Grid Infrastructure 11.2.0.3. The software components of the topology are:

- Oracle High Availability daemons running from Grid Infrastructure home.
- Single-Instance Oracle ASM running from Grid Infrastructure home.
- Single-Instance Oracle database running from an Oracle Database Oracle home.

The hardware components of the topology are:

- A database host with a public interface.
- A dedicated storage network that links to the ASM disk raid.

5.3 Provisioning and Creating Oracle Databases

This section describes about provisioning and creating Oracle Databases.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

5.3.1 Prerequisites

Before running the Deployment Procedure, meet the prerequisites listed in [Section 4.3](#).

5.3.2 Provisioning Procedure

Follow these steps:

1. Log in as a designer, and from the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the **Provision Oracle Database** Deployment Procedure and click **Launch**. The Oracle Database provisioning wizard is launched.
3. In the Select Hosts page, in the Select destination hosts section, click **Add** to select the destination host where you want to deploy and configure the software.

If you want to use a provisioning profile for the deployment, choose **Select a Provisioning Profile** and then select the profile with previously saved configuration parameters.

In the Select Tasks to Perform section, do the following:

- Select **Deploy Database software** to provision single-instance databases
- Select **Create a New Database** to create a new database and configure it after installing the standalone Oracle Database



Click on the Lock icon against the fields that you do not want to be edited in the operator role. For more information about the lock down feature in deployment procedures, see [Section 4.1](#).

Click **Next**.

4. In the Configure page, the various configuration options are displayed. Provide values for the Setup Hosts, Deploy Software, Configure Grid Infrastructure, and Create Database tasks.
5. Click on the Setup Hosts link.
6. In the Specify OS Users page, specify the operating system user for the Oracle Home for the database.

For Oracle Home User for the database, select the Normal User and Privileged User to be added to the OS group.

Click on the Lock icon against the fields that you do not want to be edited in the operator role.

Click **Next**.

7. In the Specify OS Groups page, specify the OS Groups to use for operating system authentication. Ensure that the groups corresponding to the following roles already exist on the hosts you select for provisioning.
 - Inventory Group (OINSTALL)
 - Database Administrator (OSDBA)
 - Database Operator (OSOPER)

Ensure that these groups already exist on the hosts you select for provisioning. If they do not exist, then either specify alternative groups that exist on the host or create new groups as described in Oracle Database Quick Installation Guide available at

<http://www.oracle.com/pls/db112/homepage>

The new groups you create or the alternative groups you specify automatically get SYSDBA and SYSOPER privileges after the database is configured.

For more information, see Oracle Database 2 Day DBA Guide available at:

<http://www.oracle.com/pls/db112/homepage>

Click on the Lock icon against the fields that you do not want to be edited in the operator role.

Click **Next**. You will come back to the Configure page. If you have configured the destination hosts, the Setup Hosts task will have a completed status.

8. Click on the Deploy Software link.
9. In the Select Software Locations page, specify the source and destination locations for the software binaries of Oracle Database.

In the Source section, select the Software Library location for **Oracle Database** binaries.

In the Destination location, specify the following:

- **Oracle Base for Database**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the database can be stored. This location is used for storing only the dump files

and is different from the Oracle home directory where the database software will be installed.

- **Database Oracle Home**, a location on the destination host where the database software can be provisioned. This is the Oracle home directory for the database.

In the Additional Parameters section, specify the **Working Directory** on the destination host where the files related to cloning can be staged temporarily. Ensure that you have approximately 7 GB of space for this directory. For **Installer Parameters**, specify any additional Oracle Universal Installer (OUI) parameters you want to run while provisioning Oracle database. For example, `-force` (to override any warnings), `-debug` (to view more debug information), and `-invPtrLoc <Location>` (for UNIX only). Ensure that the parameters are separated by white space.

Click on the Lock icon against the fields that you do not want to be edited in the operator role.

Click **Next**. You will come back to the Configure page. If you have configured the source and destination location for the software, the Configure Software task will have a completed status.

10. Click on the Create Databases link.
11. In the Database Template page, choose the database template location. The location can be Software Library or Oracle Home. The template selected must be compatible with the selected Oracle Home version.

If you choose **Select Template from Software Library**, click on the search icon and select the template from the Software Library. Specify **Temporary Storage Location on Managed Host(s)**. This location must exist on all hosts where you want to create the database.

Click **Show Template Details** to view details of the selected template. You can view initialization parameters, table spaces, data files, redo log groups, common options, and other details of the template.

If you choose **Select Template from Oracle Home**, select the template from the Oracle home. The default location is `ORACLE_HOME/assistants/dbca/templates`.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

12. In the Identification and Placement page, specify database configuration details. Specify **Global Database Name** and **SID** prefix. Specify the **Database Credentials** for SYS, SYSTEM, and DBSNMP database accounts. You can choose to use the same or different administrative passwords for these accounts.

Note:

- SID must be unique for a database on a host. This means, the SID assigned to one database on a host cannot be reused on another database on the same host, but can be reused on another database on a different host. For example, if you have two databases (db1 and db2) on a host (host1), then their SIDs need to be unique. However, if you install the third database on another host (host2), then its SID can be db1 or db2.
 - Global database name must be unique for a database on a host and also unique for databases across different hosts. This means, the global database name assigned to one database on a host can neither be reused on another database on the same host nor on another database on a different host. For example, if you have two databases (db1 and db2) on a host (host1), then their global database names need to be unique. And if you install the third database on another host (host2), the global database name of even this database must be unique and different from all other names registered with Cloud Control.
 - The database credentials you specify here will be used on all the destination hosts. However, after provisioning, if you want to change the password for any database, then you must change it manually.
-

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

13. In the Storage Locations page, select the storage type, whether File System or Automatic Storage Management (ASM).

If you want to use a file system, then select **File System** and specify the full path to the location where the data file is present. For example, %ORACLE_BASE%/oradata or /u01/product/db/oradata.

If you want to use ASM, then select **Automatic Storage Management (ASM)**, and click the torch icon to select the disk group name and specify ASMSNMP password. The Disk Group Name List window appears and displays the disk groups that are common on all the destination hosts.

In the Database Files Location section, specify the location where data files, temporary files, redo logs, and control files will be stored.

- Select **Use Database File Locations from Template** to select defaults from the template used.
- Select **Use Common Location for All Database Files** to specify a different location.

If you select **Use Oracle Managed Files (OMF)**, in the Multiplex Redo Logs and Control Files section, you can specify locations to store duplicate copies of redo logs and control files. Multiplexing provides greater fault-tolerance. You can specify upto five locations.

In the Recovery Files Location section, select **Use same storage type as database files location** to use the same storage type for recovery files as database files.

Select **Use Flash Recovery Area** and specify the location for recovery-related files and Fast Recovery Area Size.

Select **Enable Archiving** to enable archive logging. Click **Specify Archive Log Locations** and specify upto nine archive log locations. If the log location is not specified, the logs will be saved in the default location.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

14. In the Initialization Parameters page, select the memory management type as **Automatic Memory Management** or **Automatic Shared Memory Management**. Select **Specify Memory Settings as Percentage of Available Memory** to specify memory settings as percentage of available physical memory. For Automatic Shared Memory management, specify **Total SGA** and **Total PGA**. For Automatic Memory Management, specify **Total Memory for Oracle**.

In the Database sizing section, specify the **Block Size** and number of **Processes**. If you have selected a database template with datafiles in the Database Template page, you cannot edit the Block Size.

Specify the Host CPU Count. The maximum CPU count that can be specified is equal to the number of CPUs present on the host.

In the Character Sets section, select the default character set. The default character set is based on the locale and operating system.

Select a national character set. The default is **AL16UTF16**.

In the Database Connection Mode section, select the dedicated server mode. For shared server mode, specify the number of shared servers.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

15. In the Additional Configuration Options, all the available listeners running from the Oracle Home are listed. You can either select a listener or create a new one. You can select multiple listeners to register with the database. To create a new listener, specify the **Listener Name** and **Port**. Select database schemas and specify custom scripts, if any. Select custom scripts from the host where you are creating the database or from Software Library. If you have selected multiple hosts, you can specify scripts only from Software Library.

If you have selected a Structure Only database template in the Database Template page, you can also view and edit database options.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

16. Review the details you have provided for creating the database and click **Next**. You will come back to the Configure page. If you have configured the database, the Create Databases task will have a completed status.
17. Click the Compliance Standards link.
18. In the Configuration Standards Target Association page, select a Compliance Standard to be associated with the database. Click **Next**.

19. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure to allow me to analyze results after performing prerequisite checks** to pause the procedure execution after all prerequisite checks are performed.

Click **Next**.

20. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment.
21. In the Operator role, launch the saved deployment procedure. Add targets for provisioning and provide values for configurable fields in the deployment procedure.
22. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the Status link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.
23. After the procedure execution is completed, click on the **Targets** menu and select **All Targets** to navigate to the All Targets page and verify that the newly created databases appear as Cloud Control targets.

5.4 Provisioning Oracle Databases with Oracle Automatic Storage Management

This section describes how to provision single-instance databases with Oracle Automatic Storage Management (Oracle ASM).

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

5.4.1 Prerequisites

Before running the Deployment Procedure, meet the prerequisites listed in [Section 4.3](#).

5.4.2 Provisioning Procedure

Follow these steps:

1. Log in as a designer, and from the Enterprise menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the **Provision Oracle Database** Deployment Procedure and click **Launch**. The Oracle Database provisioning wizard is launched.
3. In the Select Hosts page, in the Select destination hosts section, click **Add** to select the destination host where you want to deploy and configure the software.

If you want to use a provisioning profile for the deployment, choose **Select a Provisioning Profile** and then select the profile with previously saved configuration parameters.

In the Select Tasks to Perform section, do the following:

- Select **Deploy Database software** to provision single-instance databases
- Select **Create a New Database** to create a new database and configure it after installing the standalone Oracle Database



Select tasks to perform 

Specify the tasks to perform as part of the provisioning process.

Deploy software

Deploy Grid Infrastructure for standalone server

Deploy Database software

Configure software

Configure Grid Infrastructure

Create a new database

Click on the Lock icon against the fields that you do not want to be edited in the operator role. For more information about the lock down feature in deployment procedures, see [Section 4.1](#).

Click **Next**.

4. In the Configure page, click on the Setup Hosts link.
5. In the Specify OS Users page, specify the operating system user for the Oracle Home for the database.

For Oracle Home User for the database, select the Normal User and Privileged User to be added to the OS group.

Click on the Lock icon against the fields that you do not want to be edited in the operator role.

Click **Next**.

6. In the Specify OS Groups page, specify the OS Groups to use for operating system authentication. Ensure that the groups corresponding to the following roles already exist on the hosts you select for provisioning.
 - Inventory Group (OINSTALL)
 - Database Administrator (OSDBA)
 - Database Operator (OSOPER)

Ensure that these groups already exist on the hosts you select for provisioning. If they do not exist, then either specify alternative groups that exist on the host or create new groups as described in Oracle Database Quick Installation Guide available at

<http://www.oracle.com/pls/db112/homepage>

The new groups you create or the alternative groups you specify automatically get SYSDBA and SYSOPER privileges after the database is configured.

For more information, see Oracle Database 2 Day DBA Guide available at:

<http://www.oracle.com/pls/db112/homepage>

Click on the Lock icon against the fields that you do not want to be edited in the operator role.

Click **Next**. You will come back to the Configure page. If you have configured the destination hosts, the Setup Hosts task will have a completed status.

7. Click on the Deploy Software link.
8. In the Select Software Locations page, specify the source and destination locations for the software binaries of Oracle Database.

In the Source section, select the Software Library location for **Oracle Database** binaries.

In the Destination location, specify the following:

- **Oracle Base for Database**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the database can be stored. This location is used for storing only the dump files and is different from the Oracle home directory where the database software will be installed.
- **Database Oracle Home**, a location on the destination host where the database software can be provisioned. This is the Oracle home directory for the database.

In the Additional Parameters section, specify the **Working Directory** on the destination host where the files related to cloning can be staged temporarily. Ensure that you have approximately 7 GB of space for this directory. For **Installer Parameters**, specify any additional Oracle Universal Installer (OUI) parameters you want to run while provisioning Oracle Grid Infrastructure. For example, `-force` (to override any warnings), `-debug` (to view more debug information), and `-invPtrLoc <Location>` (for UNIX only). Ensure that the parameters are separated by white space.

Click on the Lock icon against the fields that you do not want to be edited in the operator role.

Click **Next**. You will come back to the Configure page. If you have configured the source and destination location for the software, the Configure Software task will have a completed status.

9. Click on the Create Databases link.
10. In the Database Template page, choose the database template location. The location can be Software Library or Oracle home. The template selected must be compatible with the selected Oracle home version.

If you choose **Select Template from Software Library**, click on the search icon and select the template from the Software Library. Specify **Temporary Storage Location on Managed Host(s)**. This location must exist on all hosts where you want to create the database.

Click **Show Template Details** to view details of the selected template. You can view initialization parameters, table spaces, data files, redo log groups, common options, and other details of the template.

If you choose **Select Template from Oracle Home**, select the template from the Oracle home. The default location is `ORACLE_HOME/assistants/dbca/templates`.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

11. In the Identification and Placement page, specify database configuration details. Specify **Global Database Name** and **SID** prefix. Specify the **Database Credentials**

for SYS, SYSTEM, and DBSNMP database accounts. You can choose to use the same or different administrative passwords for these accounts.

Note:

- SID must be unique for a database on a host. This means, the SID assigned to one database on a host cannot be reused on another database on the same host, but can be reused on another database on a different host. For example, if you have two databases (db1 and db2) on a host (host1), then their SIDs need to be unique. However, if you install the third database on another host (host2), then its SID can be db1 or db2.
 - Global database name must be unique for a database on a host and also unique for databases across different hosts. This means, the global database name assigned to one database on a host can neither be reused on another database on the same host nor on another database on a different host. For example, if you have two databases (db1 and db2) on a host (host1), then their global database names need to be unique. And if you install the third database on another host (host2), the global database name of even this database must be unique and different from all other names registered with Cloud Control.
 - The database credentials you specify here will be used on all the destination hosts. However, after provisioning, if you want to change the password for any database, then you must change it manually.
-
-

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

12. In the Storage Locations page, select the storage type as **Automatic Storage Management (ASM)** and click the torch icon to select the disk group name and specify ASMSNMP password. The Disk Group Name List window appears and displays the disk groups that are common on all the destination hosts.

In the Database Files Location section, specify the location where data files, temporary files, redo logs, and control files will be stored.

- Select **Use Database File Locations from Template** to select defaults from the template used.
- Select **Use Common Location for All Database Files** to specify a different location.

If you select **Use Oracle Managed Files (OMF)**, in the Multiplex Redo Logs and Control Files section, you can specify locations to store duplicate copies of redo logs and control files. Multiplexing provides greater fault-tolerance. You can specify upto five locations.

In the Recovery Files Location section, select **Use same storage type as database files location** to use the same storage type for recovery files as database files. Select **Use Flash Recovery Area** and specify the location for recovery-related files and Fast Recovery Area Size.

Select **Enable Archiving** to enable archive logging. Click **Specify Archive Log Locations** and specify upto nine archive log locations. If the log location is not specified, the logs will be saved in the default location.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

13. In the Initialization Parameters page, select the memory management type as **Automatic Memory Management** or **Automatic Shared Memory Management**. Select **Specify Memory Settings as Percentage of Available Memory** to specify memory settings as percentage of available physical memory. For Automatic Shared Memory management, specify **Total SGA** and **Total PGA**. For Automatic Memory Management, specify **Total Memory for Oracle**.

In the Database sizing section, specify the **Block Size** and number of **Processes**. If you have selected a database template with datafiles in the Database Template page, you cannot edit the Block Size.

Specify the Host CPU Count. The maximum CPU count that can be specified is equal to the number of CPUs present on the host.

In the Character Sets section, select the default character set. The default character set is based on the locale and operating system.

Select a national character set. The default is **AL16UTF16**.

In the Database Connection Mode section, select the dedicated server mode. For shared server mode, specify the number of shared servers.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

14. In the Additional Configuration Options, all the available listeners running from the Oracle Home are listed. You can either select a listener or create a new one. You can select multiple listeners to register with the database. To create a new listener, specify the **Listener Name** and **Port**. Select database schemas and specify custom scripts, if any. Select custom scripts from the host where you are creating the database or from Software Library. If you have selected multiple hosts, you can specify scripts only from Software Library.

If you have selected a Structure Only database template in the Database Template page, you can also view and edit database options.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

15. Review the details you have provided for creating the database and click **Next**. You will come back to the Configure page. If you have configured the database, the Create Databases task will have a completed status.
16. Click the Compliance Standards link.
17. In the Configuration Standards Target Association page, select a Compliance Standard to be associated with the database. Click **Next**.
18. In the Configure page, click **Next**.

19. The Custom Properties page will be displayed only for user customized deployment procedures that require custom parameters. Specify custom properties for the deployment, if any. Click **Next**.
20. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure to allow me to analyze results after performing prerequisite checks** to pause the procedure execution after all prerequisite checks are performed.
Click **Next**.
21. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment.
22. In the Operator role, launch the saved deployment procedure. Add targets for provisioning and provide values for configurable fields in the deployment procedure.
23. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the Status link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.
24. After the procedure execution is completed, click on the **Targets** menu and select **All Targets** to navigate to the All Targets page and verify that the newly created databases appear as Cloud Control targets.

5.5 Provisioning Oracle Database Software Only

This section provides information about provisioning single-instance database software.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

5.5.1 Prerequisites

Before running the Deployment Procedure, meet the prerequisites listed in [Section 4.3](#).

5.5.2 Provisioning Procedure

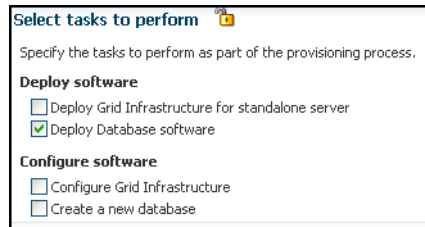
Follow these steps:

1. Log in as a designer, and from the Enterprise menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the Provision Oracle Database Deployment Procedure and click **Launch**. The Oracle Database provisioning wizard is launched.

3. In the Select Hosts page, in the Select destination hosts section, click **Add** to select the destination host where you want to deploy and configure the software.

If you want to use a provisioning profile for the deployment, choose **Select a Provisioning Profile** and then select the profile with previously saved configuration parameters.

In the Select Tasks to Perform section, select **Deploy Database software** to provision single-instance databases.



Click on the Lock icon against the fields that you do not want to be edited in the operator role. For more information about the lock down feature in deployment procedures, see [Section 4.1](#).

Click **Next**.

4. In the Configure page, click on the Setup Hosts link.
5. In the Specify OS Users page, specify the operating system user for the Oracle Home for the database.

For Oracle Home User for the database, select the Normal User and Privileged User to be added to the OS group.

Click on the Lock icon against the fields that you do not want to be edited in the operator role.

Click **Next**.

6. In the Specify OS Groups page, specify the OS Groups to use for operating system authentication. Ensure that the groups corresponding to the following roles already exist on the hosts you select for provisioning.
 - Inventory Group (OINSTALL)
 - Database Administrator (OSDBA)
 - Database Operator (OSOPER)

If these groups do not exist, then either specify alternative groups that exist on the host or create new groups as described in Oracle Database Quick Installation Guide available at:

<http://www.oracle.com/pls/db112/homepage>

The new groups you create or the alternative groups you specify automatically get SYSDBA and SYSOPER privileges after the database is configured.

For more information, see Oracle Database 2 Day DBA Guide available at:

<http://www.oracle.com/pls/db112/homepage>

Click on the Lock icon against the fields that you do not want to be edited in the operator role.

Click **Next**. You will come back to the Configure page. If you have configured the destination hosts, the Setup Hosts task will have a completed status.

7. Click on the Deploy Software link.
8. In the Select Software Locations page, specify the source and destination locations for the software binaries of Oracle Database.

In the Source section, select the Software Library location for **Oracle Database** binaries.

In the Destination location, specify the following:

- **Oracle Base for Database**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the database can be stored. This location is used for storing only the dump files and is different from the Oracle home directory where the database software will be installed.
- **Database Oracle Home**, a location on the destination host where the database software can be provisioned. This is the Oracle home directory for the database.

In the Additional Parameters section, specify the **Working Directory** on the destination host where the files related to cloning can be staged temporarily. Ensure that you have approximately 7 GB of space for this directory. For **Installer Parameters**, specify any additional Oracle Universal Installer (OUI) parameters you want to run while provisioning Oracle database. For example, `-force` (to override any warnings), `-debug` (to view more debug information), and `-invPtrLoc <Location>` (for UNIX only). Ensure that the parameters are separated by white space.

Click on the Lock icon against the fields that you do not want to be edited in the operator role.

Click **Next**. You will come back to the Configure page. If you have configured the source and destination location for the software, the Configure Software task will have a completed status.

9. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure to allow me to analyze results after performing prerequisite checks** to pause the procedure execution after all prerequisite checks are performed.

Click **Next**.

10. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment.
11. In the Operator role, launch the saved deployment procedure. Add targets for provisioning and provide values for configurable fields in the deployment procedure.
12. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the Status link for each step to view the

details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

13. After the procedure execution is completed, click on the **Targets** menu and select **All Targets** to navigate to the All Targets page and verify that the newly created databases appear as Cloud Control targets.

Provisioning Oracle Grid Infrastructure for Oracle Databases

This chapter explains how you can mass-deploy Oracle Grid Infrastructure for Oracle databases (also called as single-instance databases) in an unattended, repeatable, and reliable manner, using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Getting Started](#)
- [Provisioning Oracle Grid Infrastructure and Oracle Databases with Oracle Automatic Storage Management](#)
- [Provisioning Oracle Grid Infrastructure and Oracle Database Software Only](#)

6.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in provisioning Oracle Grid Infrastructure for single-instance databases. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision Oracle Grid Infrastructure with single-instance databases. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 6–1 *Getting Started with Provisioning Oracle Grid Infrastructure*

Step	Description	Reference Links
Step 1	<p>Selecting the Use Case</p> <p>This chapter covers a few use cases for provisioning Oracle Grid Infrastructure. Select the use case that best matches your requirement.</p>	<ul style="list-style-type: none"> ■ To learn about provisioning Grid Infrastructure and Oracle databases and configuring database with Oracle ASM, see Section 6.2. ■ To learn about provisioning Grid Infrastructure and Oracle database software only, see Section 6.3.
Step 2	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	<ul style="list-style-type: none"> ■ To learn about the prerequisites for provisioning Grid Infrastructure and Oracle databases and configuring database with Oracle ASM, see Section 6.2.1. ■ To learn about the prerequisites for provisioning Grid Infrastructure and single-instance database software only, see Section 6.3.1.

Table 6–1 (Cont.) Getting Started with Provisioning Oracle Grid Infrastructure

Step	Description	Reference Links
Step 3	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully provision Oracle Grid Infrastructure.</p>	<ul style="list-style-type: none"> ■ To provision Grid Infrastructure and Oracle databases and configuring database with Oracle ASM, follow the steps explained in Section 6.2.2. ■ To provision Grid Infrastructure and Oracle database software only, follow the steps explained in Section 6.3.2.

6.2 Provisioning Oracle Grid Infrastructure and Oracle Databases with Oracle Automatic Storage Management

This section describes how you can provision Oracle Grid Infrastructure and single-instance databases with Oracle Automatic Storage Management (ASM).

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

6.2.1 Prerequisites

Before running the Deployment Procedure, meet the prerequisites listed in [Section 4.3](#).

6.2.2 Provisioning Procedure

Follow these steps:

1. Log in as a designer, and from the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the Provision Oracle Database Deployment Procedure and click **Launch**. The Oracle Database provisioning wizard is launched.
3. In the Select Hosts page, in the Select destination hosts section, click **Add** to select the destination host where you want to deploy and configure the software.

If you want to use a provisioning profile for the deployment, choose **Select a Provisioning Profile** and then select the profile with previously saved configuration parameters.

In the Select Tasks to Perform section, do the following:

- Select **Deploy Grid Infrastructure for standalone server** to provision Grid Infrastructure
- Select **Deploy Database software** to provision single-instance databases
- Select **Configure Grid Infrastructure** to configure Grid Infrastructure
- Select **Create a new database** to create a new database and configure it after installing the standalone Oracle Database

Select tasks to perform

Specify the tasks to perform as part of the provisioning process.

Deploy software

- Deploy Grid Infrastructure for standalone server
- Deploy Database software

Configure software

- Configure Grid Infrastructure
- Create a new database

Click on the Lock icon against the fields that you do not want to be edited in the operator role. For more information about the lock down feature in deployment procedures, see [Section 4.1](#).

Click **Next**.

4. In the Configure page, click on the Setup Hosts link.
5. In the Specify OS Users page, specify the operating system user for the Oracle Home for the database and Grid Infrastructure. Specify the Normal User and Privileged User to be added to the OS groups.

Click **Next**.

6. In the Specify OS Groups page, specify the OS Groups to use for operating system authentication. Ensure that the groups corresponding to the following roles already exist on the hosts you select for provisioning.
 - Inventory Group (OINSTALL)
 - Database Administrator (OSDBA)
 - Database Operator (OSOPER)
 - ASM Instance Administrator (OSASM)
 - ASM Database Administrator (ASMDBA)
 - ASM Instance Operator (ASMOPER)

If they do not exist, then either specify alternative groups that exist on the host or create new groups as described in Oracle Database Quick Installation Guide available at

<http://www.oracle.com/pls/db112/homepage>

The new groups you create or the alternative groups you specify automatically get SYSDBA and SYSOPER privileges after the database is configured.

For more information, see Oracle Database 2 Day DBA Guide available at:

<http://www.oracle.com/pls/db112/homepage>

Click **Next**. You will come back to the Configure page. If you have configured the destination hosts, the Setup Hosts task will have a completed status.

7. Click on the Deploy Software link.
8. In the Select Software Locations page, specify the source and destination locations for the software binaries of Oracle Database.

In the Source section, select the Software Library location for the **Grid Infrastructure** and **Oracle Database** binaries.

In the Destination location, specify the following:

- **Oracle Base for Grid Infrastructure**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the Grid Infrastructure can be stored.
- **Grid Infrastructure Home**, a location on the destination host where the Grid Infrastructure software can be provisioned. This is the Oracle home directory for Grid Infrastructure. Do not select a location that is a subdirectory of the Oracle Base for Grid Infrastructure or database.
- **Oracle Base for Database**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the database can be stored. This location is used for storing only the dump files and is different from the Oracle home directory where the database software will be installed.
- **Database Oracle Home**, a location on the destination host where the database software can be provisioned. This is the Oracle home directory for the database.

For Grid Infrastructure, Oracle Base is `/u01/app/user` and Oracle Home is `%ORACLE_BASE%/sihome`. You can use `%ORACLE_BASE%` and `%GI_ORACLE_BASE%` to specify the relative paths which will be interpolated to their respective values.

In the Additional Parameters section, specify the **Working Directory** on the destination host where the files related to cloning can be staged temporarily. Ensure that you have approximately 7 GB of space for this directory. For **Installer Parameters**, specify any additional Oracle Universal Installer (OUI) parameters you want to run while provisioning Oracle Grid Infrastructure. For example, `-force` (to override any warnings), `-debug` (to view more debug information), and `-invPtrLoc <Location>` (for UNIX only). Ensure that the parameters are separated by white space.

Click on the Lock icon against the fields that you do not want to be edited in the operator role.

Click **Next**. You will come back to the Configure page. If you have configured the source and destination location for the software, the Configure Software task will have a completed status.

9. Click on the Configure Grid Infrastructure link.
10. In the Configure GI page, in the ASM Storage section, click **Add** to add an ASM Disk Group. In the Add/Edit Disk Group dialog box, specify the **Disk Group Name**, **Disk List**, and specify the redundancy as **Normal**, **High**, or **External**. Click **OK**.

For ASM 11.2 and higher, specify the **Disk Group Name** for storing the parameter file. Specify the **ASM Password** for ASMSNMP and SYS users. Specify the Listener Port for registering the ASM instances.

As a designer, you can click on the Lock icon to lock these fields. These fields will then not be available for editing in the operator role.

Click **Next**. You will come back to the Configure page. If you have configured the storage options for the Grid Infrastructure and database, the Configure Grid Infrastructure task will have a completed status.

11. Click on the Create Databases link.
12. In the Database Template page, choose the database template location. The location can be Software Library or Oracle home. The template selected must be compatible with the selected Oracle home version.

If you choose **Select Template from Software Library**, click on the search icon and select the template from the Software Library. Specify **Temporary Storage Location on Managed Host(s)**. This location must exist on all hosts where you want to create the database.

Click **Show Template Details** to view details of the selected template. You can view initialization parameters, table spaces, data files, redo log groups, common options, and other details of the template.

If you choose **Select Template from Oracle Home**, select the template from the Oracle home. The default location is `ORACLE_HOME/assistants/dbca/templates`.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

13. In the Identification and Placement page, specify database configuration details. Specify **Global Database Name** and **SID** prefix. Specify the **Database Credentials** for SYS, SYSTEM, and DBSNMP database accounts. You can choose to use the same or different administrative passwords for these accounts.

Note:

- SID must be unique for a database on a host. This means, the SID assigned to one database on a host cannot be reused on another database on the same host, but can be reused on another database on a different host. For example, if you have two databases (db1 and db2) on a host (host1), then their SIDs need to be unique. However, if you install the third database on another host (host2), then its SID can be db1 or db2.
 - Global database name must be unique for a database on a host and also unique for databases across different hosts. This means, the global database name assigned to one database on a host can neither be reused on another database on the same host nor on another database on a different host. For example, if you have two databases (db1 and db2) on a host (host1), then their global database names need to be unique. And if you install the third database on another host (host2), the global database name of even this database must be unique and different from all other names registered with Cloud Control.
 - The database credentials you specify here will be used on all the destination hosts. However, after provisioning, if you want to change the password for any database, then you must change it manually.
-
-

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

14. In the Storage Locations page, select the storage type as **Automatic Storage Management (ASM)**, and click the torch icon to select the disk group name and specify ASMSNMP password. The Disk Group Name List window appears and displays the disk groups that are common on all the destination hosts.

In the Database Files Location section, specify the location where data files, temporary files, redo logs, and control files will be stored.

- Select **Use Database File Locations from Template** to select defaults from the template used.
- Select **Use Common Location for All Database Files** to specify a different location.

If you select **Use Oracle Managed Files (OMF)**, in the Multiplex Redo Logs and Control Files section, you can specify locations to store duplicate copies of redo logs and control files. Multiplexing provides greater fault-tolerance. You can specify up to five locations.

In the Recovery Files Location section, select **Use same storage type as database files location** to use the same storage type for recovery files as database files. Select **Use Flash Recovery Area** and specify the location for recovery-related files and Fast Recovery Area Size.

Select **Enable Archiving** to enable archive logging. Click **Specify Archive Log Locations** and specify up to nine archive log locations. If the log location is not specified, the logs will be saved in the default location.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

15. In the Initialization Parameters page, select the memory management type as **Automatic Memory Management** or **Automatic Shared Memory Management**. Select **Specify Memory Settings as Percentage of Available Memory** to specify memory settings as percentage of available physical memory. For Automatic Shared Memory management, specify **Total SGA** and **Total PGA**. For Automatic Memory Management, specify **Total Memory for Oracle**.

In the Database sizing section, specify the **Block Size** and number of **Processes**. If you have selected a database template with datafiles in the Database Template page, you cannot edit the Block Size.

Specify the Host CPU Count. The maximum CPU count that can be specified is equal to the number of CPUs present on the host.

In the Character Sets section, select the default character set. The default character set is based on the locale and operating system.

Select a national character set. The default is **AL16UTF16**.

In the Database Connection Mode section, select the dedicated server mode. For shared server mode, specify the number of shared servers.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

16. In the Additional Configuration Options, all the available listeners running from the Oracle Home are listed. You can either select a listener or create a new one. You can select multiple listeners to register with the database. To create a new listener, specify the **Listener Name** and **Port**. Select database schemas and specify custom scripts, if any. Select custom scripts from the host where you are creating the database or from Software Library. If you have selected multiple hosts, you can specify scripts only from Software Library.

If you have selected a Structure Only database template in the Database Template page, you can also view and edit database options.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

17. Review the details you have provided for creating the database and click **Next**. You will come back to the Configure page. If you have configured the database, the Create Databases task will have a completed status.
18. Click the Compliance Standards link.
19. In the Configuration Standards Target Association page, select a Compliance Standard to be associated with the database. Click **Next**.
20. The Custom Properties page will be displayed only for user customized deployment procedures that require custom parameters. Specify custom properties for the deployment, if any. Click **Next**.
21. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure to allow me to analyze results after performing prerequisite checks** to pause the procedure execution after all prerequisite checks are performed.

Click **Next**.

22. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment.
23. In the Operator role, launch the saved deployment procedure. Add targets for provisioning and provide values for configurable fields in the deployment procedure.
24. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the Status link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.
25. After the procedure execution is completed, click on the **Targets** menu and select **All Targets** to navigate to the All Targets page and verify that the newly provisioned databases appear as Cloud Control targets.

Note: if the Deployment Procedure fails, then review log files described in [Section E.8](#).

6.3 Provisioning Oracle Grid Infrastructure and Oracle Database Software Only

This section describes how you can provision Oracle Grid Infrastructure and Oracle Database software.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

6.3.1 Prerequisites

Before running the Deployment Procedure, meet the prerequisites listed in [Section 4.3](#).

6.3.2 Provisioning Procedure

To provision Oracle Grid Infrastructure and Oracle Database software, follow these steps:

1. Log in as a designer, and from the Enterprise menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the Oracle Database Deployment Procedure and click **Launch**. The Oracle Database provisioning wizard is launched.
3. In the Select Hosts page, in the Select destination hosts section, click **Add** to select the destination host where you want to deploy and configure the software.

If you want to use a provisioning profile for the deployment, choose **Select a Provisioning Profile** and then select the profile with previously saved configuration parameters.

In the Select Tasks to Perform section, do the following:

- Select **Deploy Grid Infrastructure for standalone server** to provision Grid Infrastructure
- Select **Deploy Database software** to provision single-instance databases

Click on the Lock icon against the fields that you do not want to be edited in the operator role. For more information about the lock down feature in deployment procedures, see [Section 4.1](#).

Click **Next**.

4. In the Configure page, click on the Setup Hosts link.
5. In the Specify OS Users page, specify the operating system user for the Oracle Home for the database and Grid Infrastructure. Specify the Normal User and Privileged User to be added to the OS groups.

Click **Next**.

6. In the Specify OS Groups page, specify the OS Groups to use for operating system authentication. Ensure that the groups corresponding to the following roles already exist on the hosts you select for provisioning.
 - Inventory Group (OINSTALL)
 - Database Administrator (OSDBA)
 - Database Operator (OSOPER)
 - ASM Instance Administrator (OSASM)
 - ASM Database Administrator (ASMDBA)
 - ASM Instance Operator (ASMOPER)

If they do not exist, then either specify alternative groups that exist on the host or create new groups as described in Oracle Database Quick Installation Guide available at

<http://www.oracle.com/pls/db112/homepage>

The new groups you create or the alternative groups you specify automatically get SYSDBA and SYSOPER privileges after the database is configured.

For more information, see Oracle Database 2 Day DBA Guide available at:

<http://www.oracle.com/pls/db112/homepage>

Click **Next**. You will come back to the Configure page. If you have configured the destination hosts, the Setup Hosts task will have a completed status.

7. Click on the Deploy Software link.
8. In the Select Software Locations page, specify the source and destination locations for the software binaries of Oracle Database.

In the Source section, select the Software Library location for the **Grid Infrastructure** and **Oracle Database** binaries.

In the Destination location, specify the following:

- **Oracle Base for Grid Infrastructure**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the Grid Infrastructure can be stored.
- **Grid Infrastructure Home**, a location on the destination host where the Grid Infrastructure software can be provisioned. This is the Oracle home directory for Grid Infrastructure. Do not select a location that is a subdirectory of the Oracle Base for Grid Infrastructure or database.
- **Oracle Base for Database**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the database can be stored. This location is used for storing only the dump files and is different from the Oracle home directory where the database software will be installed.
- **Database Oracle Home**, a location on the destination host where the database software can be provisioned. This is the Oracle home directory for the database.

For Grid Infrastructure, Oracle Base is `/u01/app/user` and Oracle Home is `%ORACLE_BASE%/sihome`. You can use `%ORACLE_BASE%` and `%GI_ORACLE_BASE%` to specify the relative paths which will be interpolated to their respective values.

In the Additional Parameters section, specify the **Working Directory** on the destination host where the files related to cloning can be staged temporarily. Ensure that you have approximately 7 GB of space for this directory. For **Installer Parameters**, specify any additional Oracle Universal Installer (OUI) parameters you want to run while provisioning Oracle Grid Infrastructure. For example, `-force` (to override any warnings), `-debug` (to view more debug information), and `-invPtrLoc <Location>` (for UNIX only). Ensure that the parameters are separated by white space.

Click on the Lock icon against the fields that you do not want to be edited in the operator role.

Click **Next**. You will come back to the Configure page. If you have configured the source and destination location for the software, the Configure Software task will have a completed status.

9. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure to allow me to analyze results after performing prerequisite checks** to pause the procedure execution after all prerequisite checks are performed.

Click **Next**.

10. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment.
11. In the Operator role, launch the saved deployment procedure. Add targets for provisioning and provide values for configurable fields in the deployment procedure.
12. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the Status link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

Note: if the Deployment Procedure fails, then review log files described in [Section E.8](#).

Provisioning Oracle Grid Infrastructure for Oracle Real Application Clusters Databases

This chapter explains how you can mass-deploy Oracle Grid Infrastructure and Oracle Real Application Clusters (Oracle RAC) for clustered environments in an unattended, repeatable, and reliable manner. In particular, this chapter covers the following:

- [Getting Started](#)
- [Provisioning Grid Infrastructure with Oracle Real Application Clusters Database and Configuring Database with Oracle Automatic Storage Management](#)
- [Provisioning Oracle Real Application Clusters Database with File System on an Existing Cluster](#)
- [Provisioning Oracle Real Application Clusters Database with File System on a New Cluster](#)

Note: To view an online demonstration of this feature, access the following URL:

<http://www.oracle.com/technology/obe/demos/admin/demos.html>

7.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in provisioning Oracle Grid Infrastructure and Oracle RAC. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision Oracle Grid Infrastructure and Oracle RAC. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 7–1 *Getting Started with Provisioning Oracle Grid Infrastructure and Oracle RAC Databases*

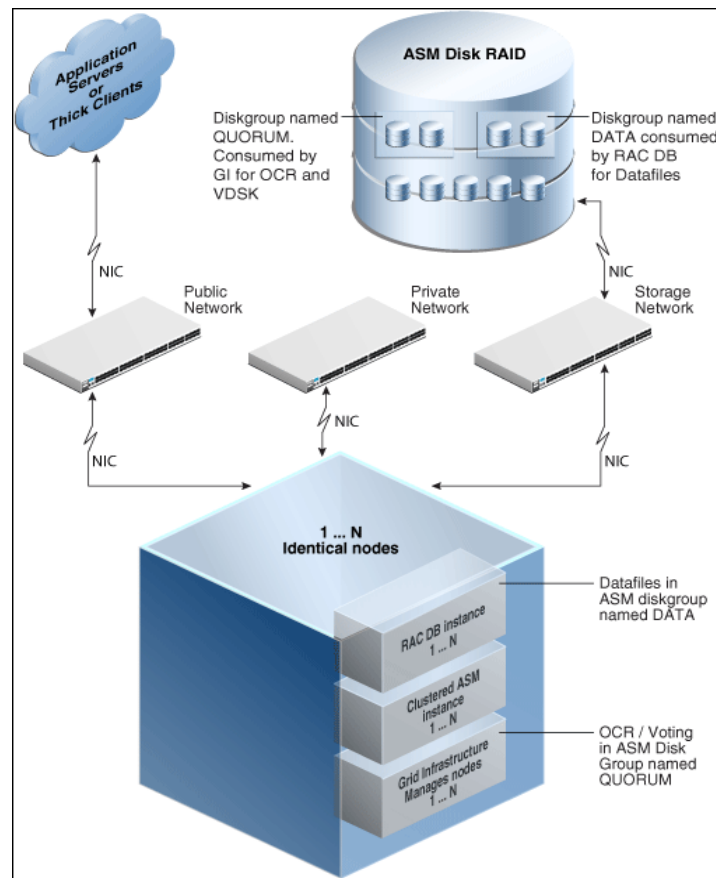
Step	Description	Reference Links
Step 1	<p>Understanding Oracle RAC Topology</p> <p>Understand the Oracle Real Application Clusters Database topology provisioned by Cloud Control.</p>	To learn about the topology, see Section 7.2 .

Table 7–1 (Cont.) Getting Started with Provisioning Oracle Grid Infrastructure and Oracle RAC Databases

Step	Description	Reference Links
Step 2	<p>Selecting the Use Case</p> <p>This chapter covers a few use cases for provisioning Oracle Grid Infrastructure and Oracle RAC. Select the use case that best matches your requirement.</p>	<ul style="list-style-type: none"> ■ To learn about provisioning Oracle Grid Infrastructure and Oracle RAC database and configuring ASM and Database, see Section 7.3. ■ To learn about provisioning Oracle RAC database with File System on an existing cluster, see Section 7.4. ■ To learn about provisioning Oracle RAC database with File System on a new cluster, see Section 7.5.
Step 3	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	<ul style="list-style-type: none"> ■ To learn about the prerequisites for provisioning Oracle Grid Infrastructure and Oracle RAC database and configuring ASM and Database, see Section 7.3.1. ■ To learn about the prerequisites for provisioning Oracle RAC database with File System on an existing cluster, see Section 7.4.1. ■ To learn about the prerequisites for provisioning Oracle RAC database with File System on a new cluster, see Section 7.5.1.
Step 4	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully provision Oracle Grid Infrastructure and Oracle RAC.</p>	<ul style="list-style-type: none"> ■ To provision Oracle Grid Infrastructure and Oracle RAC database and configure ASM and Database, follow the steps explained in Section 7.3.2. ■ To provision Oracle RAC database with File System on an existing cluster, follow the steps explained in Section 7.4.2. ■ To provision Oracle RAC database with File System on a new cluster, follow the steps explained in Section 7.5.2.

7.2 Oracle Real Application Clusters Database Topology

Oracle Enterprise Manager Cloud Control enables standardized gold image-based deployments of Oracle RAC databases with provisioning profiles, input lock down in designer role, and associating compliance standards with databases. [Figure 7–1](#) shows a typical Oracle RAC database topology that you can provision using Cloud Control.

Figure 7-1 Oracle RAC Database Topology

The topology shows a N-node setup using Grid Infrastructure, clustered ASM, and policy-managed Oracle RAC database. An ASM disk array is shared through the cluster setup. The Grid Infrastructure uses an ASM diskgroup named QUORUM for Oracle Cluster Registry (OCR) and Voting Disk (Heartbeat). The Oracle RAC database uses another diskgroup named DATA. This stores database datafiles. The nodes are multihomed such that a high speed internal network between nodes facilitates cluster operation and a public network is used for external connectivity. The networks are public, private, and storage network between nodes and the ASM disk array.

7.3 Provisioning Grid Infrastructure with Oracle Real Application Clusters Database and Configuring Database with Oracle Automatic Storage Management

This section describes how you can provision Grid Infrastructure with Oracle RAC Database and configure Database with Oracle ASM.

In particular, this section covers the following:

- [Prerequisites](#)
- [Procedure](#)

7.3.1 Prerequisites

Before running the Deployment Procedure, meet the prerequisites listed in [Section 4.3](#).

7.3.2 Procedure

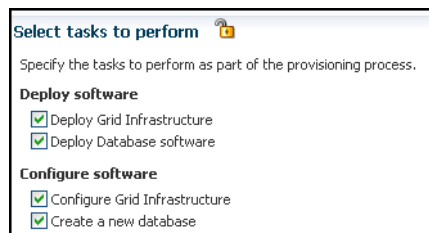
Follow these steps:

1. Log in as a designer, and from the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the Provision Oracle RAC Database Deployment Procedure and click **Launch**. The Oracle RAC Database provisioning wizard is launched.
3. In the Select Hosts page, select the provisioning and configuration actions and destination hosts.

If you want to use a provisioning profile for the deployment, choose **Select a Provisioning Profile** and then select the profile with previously saved configuration parameters.

In the Select Tasks to Perform section, do the following:

- Select **Deploy Grid Infrastructure** to provision Grid Infrastructure
- Select **Deploy Database software** to provision Oracle RAC databases
- Select **Configure Grid Infrastructure** to configure Grid Infrastructure
- Select **Create a New Database** to create and configure the database



In the Select destination hosts section, click **Add** to select the destination host where you want to deploy and configure the Grid Infrastructure and database.

Click on the Lock icon against the fields that you do not want to be edited in the operator role. For more information about the lock down feature in deployment procedures, see [Section 4.1](#).

Click **Next**.

4. In the Configure page, click on the Setup Hosts link.
5. In the Specify OS Users page, specify the operating system users and groups required to provision the database.

For Database User and ASM User, select the Normal User and Privileged User to be added to the OS group.

Click **Next**.

6. In the Specify OS Groups page, specify the OS Groups to use for operating system authentication. Ensure that the groups corresponding to the following roles already exist on the hosts you select for provisioning.
 - Inventory Group (OINSTALL)
 - ASM Database Administrator (ASMDBA)
 - ASM Instance Operator (ASMOPER)

- Database Administrator (OSDBA)
- Database Operator (OSOPER)
- ASM Instance Administrator (OSASM)

Click **Next**. You will come back to the Configure page. If you have configured the destination hosts, the Setup Hosts task will have a Configured status.

7. Click on the Deploy Software link.
8. In the Select Software Locations page, specify the locations where the software binaries of Oracle Grid Infrastructure and Oracle RAC can be placed, that is, the \$ORACLE_HOME location. As a designer, you can click on the Lock icon to lock these fields. These fields will then not be available for editing in the operator role.

In the Source section, select the Software Library location for the **Grid Infrastructure** and **Oracle Database** binaries.

In the Destination location, specify the following:

- **Oracle Base for Grid Infrastructure**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the Grid Infrastructure can be stored.
- **Grid Infrastructure Home**, a location on the destination host where the Grid Infrastructure software can be provisioned. This is the Oracle home directory for Grid Infrastructure. Do not select a location that is a subdirectory of the Oracle Base for Grid Infrastructure or database. Select **Shared Grid Infrastructure home** to enable Grid Infrastructure Oracle Home on shared locations. Ensure that the directory path you provide meets the requirements described in [Section 7.3.2.1](#).
- **Oracle Base for Database**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the database can be stored. This location is used for storing only the dump files and is different from the Oracle home directory where the database software will be installed.
- **Database Oracle Home**, a location on the destination host where the database software can be provisioned. This is the Oracle home directory for the database. Select **Shared Database Oracle home** to enable Database Oracle Home on shared locations.

For Grid Infrastructure, Oracle Base is /u01/app/user and Oracle Home is %ORACLE_BASE/../../grid. You can use %ORACLE_BASE% and %GI_ORACLE_BASE% to specify the relative paths which will be interpolated to their respective values.

In the Additional Parameters section, specify the **Working Directory** on the destination host where the files related to cloning can be staged temporarily. Ensure that you have approximately 7 GB of space for this directory. For **Installer Parameters**, specify any additional Oracle Universal Installer (OUI) parameters you want to run while provisioning Oracle Grid Infrastructure. For example, -force (to override any warnings), -debug (to view more debug information), and -invPtrLoc <Location> (for UNIX only). Ensure that the parameters are separated by white space.

You can also specify OCFS devices in the Installer Parameters field in the following format, separating devices with commas:

```
Device Number:Partition Number: Drive letter: [DATA | SOFTWARE]
```

For example:

Click **Next**. You will come back to the Configure page. If you have configured the source and destination location for the software, the Configure Software task will have a Configured status.

9. Click on the Configure Grid Infrastructure link.
10. In the Select Storage page, select the storage type for Grid Infrastructure and database as **Automatic Storage Management** or **File System** to indicate the storage type for storing voting disk and Oracle Cluster Registry (OCR). Voting disk and OCR are used by Oracle Clusterware to manage its resources. You can choose from the following options:
 - Automatic Storage Management for both Grid Infrastructure and Oracle RAC Database
 - Automatic Storage Management for Grid Infrastructure and File System for Oracle RAC Database
 - File System for both Grid Infrastructure and Oracle RAC Database
 - File System for Grid Infrastructure and Automatic Storage Management for Oracle RAC Database

As a designer, you can click on the Lock icon to lock these fields. These fields will then not be available for editing in the operator role.

Click **Next**.

11. In the Configure GI page, in the Basic Settings section, specify the **Cluster Name**, **SCAN Name**, and **SCAN Port**. The default SCAN port is port 1521, but you can specify another port of your choice. The deployment procedure verifies that the SCAN port provided is a valid port number, and is not used for any other purpose. After installation, a TNS listener listens to this port to respond to client connections to the SCAN name.

Configure Grid Infrastructure **Select Storage** **Configure GI** Configure Grid Infrastructure

Provision Oracle RAC Database : Configure GI

Basic Settings

Cluster Name

SCAN Name

SCAN Port

GNS Settings

Configure GNS

GNS Sub System

GNS VIP Address

GI Network

Add Delete...

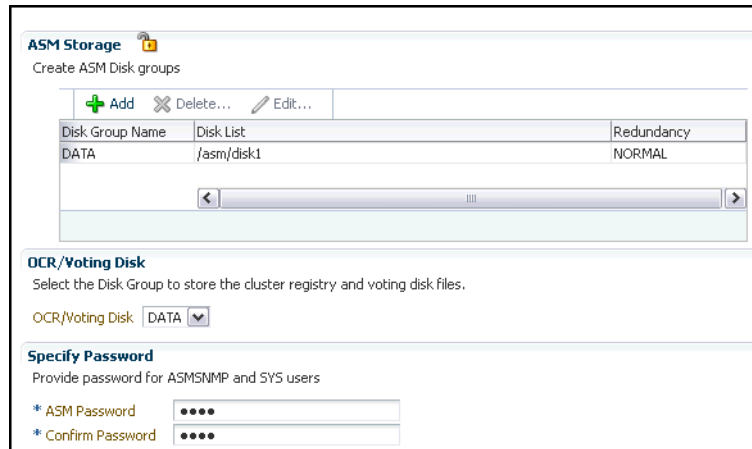
Interface Name	Interface Subnet	Usage
eth0	140.84.128.0	PUBLIC

In the GNS Settings section, select **Configure GNS** and **auto-assign with DHCP** and specify the **GNS Sub System** and **GNS VIP Address** if you want virtual host names outside the cluster to have dynamically assigned names.

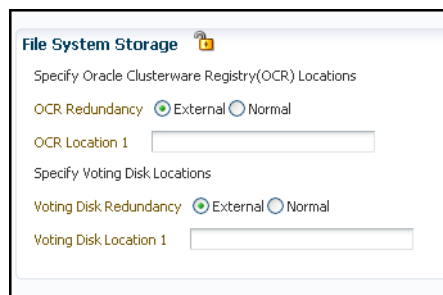
In the GI Network section, by default, the network interfaces that have the same name and subnet for the selected destination hosts are automatically detected and displayed. Validate these network interface configuration details. From the Usage column, select **Public** to configure the interface as public interface, or **Private** to configure the interface as private interface.

Click **Add** to add an interface and specify the **Interface Name** and **Interface Subnet** and click **OK**. Select the Usage as **Public**, **Private**, or **Do Not Use** if you do not want to use the interface.

If you have chosen storage type as Automatic Storage Management for either or both Grid Infrastructure and Oracle RAC Database, in the ASM Storage section, select from the ASM Disk Groups that have been discovered by Cloud Control and are displayed in the table. Click **Add** to add an ASM Disk Group. In the Add/Edit Disk Group dialog box, specify the **Disk Group Name**, **Disk List**, and specify the redundancy as **Normal**, **High**, or **External**. Click **OK**. Select the OCR/Voting Disk to store cluster registry and voting disk files, and specify the ASM credentials for ASMSNMP and SYS users.



If you have chosen storage type as File System for Grid Infrastructure or Oracle RAC database, in the File System Storage section, specify the storage location for Oracle Cluster Registry (OCR) and voting disks. Select Normal or External to indicate the redundancy level, and specify their locations.



As a designer, you can click on the Lock icon to lock these fields. These fields will then not be available for editing in the operator role.

Click **Next**. You will come back to the Configure page. If you have configured the storage options for the Grid Infrastructure and database, the Configure Grid Infrastructure task will have a completed status.

12. Click on the Create Databases link.
13. In the Database Template page, choose the database template location. The location can be Software Library or Oracle home. The template selected must be compatible with the selected Oracle home version.

If you have selected **Software Library**, click on the search icon and select the template from the Software Library. Specify **Temporary Storage Location on Managed Host(s)**. This location must be present on the reference node that you selected earlier.

Click **Show Template Details** to view details of the selected template. You can view initialization parameters, table spaces, data files, redo log groups, common options, and other details of the template.

If you have selected **Oracle Home**, select the template from the Oracle home. The default location is ORACLE_HOME/assistants/dbca/templates.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

14. In the Identification and Placement page, select the Oracle RAC database configuration type, whether Policy Managed or Admin Managed.

For admin-managed database, select nodes on which you want to create the cluster database. You must specify the node selected as the reference node in the Database Version and Type page.

For policy-managed database, select the server pools to be used for creating the database, from the list of existing server pools, or choose to create a new server pool. Policy-managed databases can be created for database versions 11.2 and higher. For database versions lower than 11.2, you will need to select nodes to create the Oracle RAC database.

Specify **Global Database Name** and **SID** prefix. Specify the **Database Credentials** for SYS, SYSTEM, and DBSNMP. You can choose to specify the same or different passwords for each of these user accounts.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

15. In the Storage Locations page, select the same storage type you specified for Oracle Database in the Select Storage page.

In the Database Files Location section, specify the location where data files, temporary files, redo logs, and control files will be stored. These locations must be on shared storage such as cluster file system location or ASM diskgroups.

- Select **Use Database File Locations from Template** to select defaults from the template used.
- Select **Use Common Location for All Database Files** to specify a different location.

If you select **Use Oracle Managed Files (OMF)**, in the Multiplex Redo Logs and Control Files section, you can specify locations to store duplicate copies of redo logs and control files. Multiplexing provides greater fault-tolerance. You can specify upto five locations.

In the Recovery Files Location section, select **Use same storage type as database files location** to use the same storage type for recovery files as database files. Select **Use Flash Recovery Area** and specify the location for recovery-related files and Fast Recovery Area Size.

Select **Enable Archiving** to enable archive logging. Click **Specify Archive Log Locations** and specify upto nine archive log locations. If the log location is not specified, the logs will be saved in the default location.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

16. In the Initialization Parameters page, select the memory management type as **Automatic Memory Management** or **Automatic Shared Memory Management**. Select **Specify Memory Settings as Percentage of Available Memory** to specify memory settings as percentage of available physical memory. For Automatic Shared Memory management, specify **Total SGA** and **Total PGA**. For Automatic Memory Management, specify **Total Memory for Oracle**.

In the Database sizing section, specify the **Block Size** and number of **Processes**. If you have selected a database template with datafiles in the Database Template page, you cannot edit the Block Size.

Specify the Host CPU Count. The maximum CPU count that can be specified is equal to the number of CPUs present on the host.

In the Character Sets section, select the default character set. The default character set is based on the locale and operating system.

Select a national character set. The default is **AL16UTF16**.

In the Database Connection Mode section, select the dedicated server mode. For shared server mode, specify the number of shared servers.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

17. In the Additional Configuration Options page, select custom scripts from the Software Library or your local disk. If you have selected a Structure Only database template in the Database Template page, you can also view and edit database options.

Click on the Lock icon to lock the field. Click **Next**.

18. Review the information you have provided and click **Next**. You will come back to the Configure page. If you have configured the database, the Create Databases task will have a Configured status. Click **Next**.

19. Click the Compliance Standards link.

20. In the Configuration Standards Target Association page, select a Compliance Standard to be associated with the database. Click **Next**.

21. In the Configure page, click **Next**.

22. The Custom Properties page will be displayed only for user customized deployment procedures that require custom parameters. Specify custom properties for the deployment, if any. Click **Next**.

23. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure to allow me to analyze results after performing prerequisite checks** to pause the procedure execution after all prerequisite checks are performed.

Click **Next**.

24. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment.

25. In the Operator role, launch the saved deployment procedure. Add targets for provisioning and provide values for configurable fields in the deployment procedure.

26. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the Status link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.
27. After the procedure execution is completed, click on the **Targets** menu and select **All Targets** to navigate to the All Targets page and verify that the newly provisioned databases appear as Cloud Control targets.

Note: if the Deployment Procedure fails, then review log files described in [Section E.8](#).

7.3.2.1 Requirements for Grid Infrastructure Software Location Path

Meet the following requirements while specifying a directory path for the Oracle Grid Infrastructure home to deploy the Oracle Grid Infrastructure binaries:

- It should be created in a path outside existing Oracle homes
- It should not be located in a user home directory
- It should be created either as a subdirectory in a path where all files can be owned by root, or in a unique path
- Before installation, it should be owned by the installation owner of Oracle Grid Infrastructure (typically, `oracle`, for a single installation owner for all Oracle software, or `grid` for role-based Oracle installation owners), and set to 755 permissions

7.4 Provisioning Oracle Real Application Clusters Database with File System on an Existing Cluster

In particular, this section covers the following:

- [Prerequisites](#)
- [Procedure](#)

7.4.1 Prerequisites

Before running the Deployment Procedure, meet the prerequisites listed in [Section 4.3](#).

7.4.2 Procedure

To provision Oracle RAC databases with file system on an existing cluster, follow these steps:

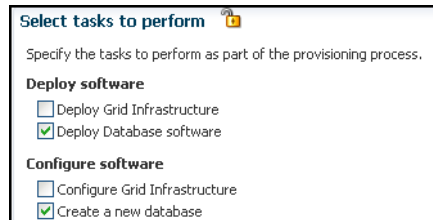
Follow these steps:

1. Log in as a designer, and from the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the Provision Oracle RAC Database Deployment Procedure and click **Launch**. The Oracle RAC Database provisioning wizard is launched.
3. In the Select Hosts page, select the provisioning and configuration actions and destination hosts.

If you want to use a provisioning profile for the deployment, choose **Select a Provisioning Profile** and then select the profile with previously saved configuration parameters.

In the Select Tasks to Perform section, do the following:

- Select **Deploy Oracle Database Software** to provision Oracle RAC database software
- Select **Create a New Database** to create and configure the database



In the Select destination hosts section, click **Add** to select the cluster on which you want to deploy the Grid Infrastructure and configure the database.

Click on the Lock icon against the fields that you do not want to be edited in the operator role. For more information about the lock down feature in deployment procedures, see [Section 4.1](#).

Click **Next**.

4. In the Configure page, click on the Setup Hosts link.
5. In the Specify OS Users page, specify the operating system users and groups required to provision the database.

For Database User, select the Normal User and Privileged User to be added to the OS group.

Click **Next**.

6. In the Specify OS Groups page, specify the OS Groups to use for operating system authentication. Ensure that the groups corresponding to the following roles already exist on the hosts you select for provisioning.
 - Inventory Group (OINSTALL)
 - Database Administrator (OSDBA)
 - Database Operator (OSOPER)

Click **Next**. You will come back to the Configure page. If you have configured the destination hosts, the Setup Hosts task will have a Configured status.

7. Click on the Deploy Software link.
8. In the Select Software Locations page, specify the locations where the software binaries of Oracle RAC database can be placed, that is, the \$ORACLE_HOME location. As a designer, you can click on the Lock icon to lock these fields. These fields will then not be available for editing in the operator role.

In the Source section, select the Software Library location for the **Grid Infrastructure** and **Oracle Database** binaries.

In the Destination location, specify the following:

- **Oracle Base for Database**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the database can be stored. This location is used for storing only the dump files and is different from the Oracle home directory where the database software will be installed.
- **Database Oracle Home**, a location on the destination host where the database software can be provisioned. This is the Oracle home directory for the database. Select **Shared Database Oracle home** to enable Database Oracle Home on shared locations.

In the Additional Parameters section, specify the **Working Directory** on the destination host where the files related to cloning can be staged temporarily. Ensure that you have approximately 7 GB of space for this directory. For **Installer Parameters**, specify any additional Oracle Universal Installer (OUI) parameters you want to run while provisioning Oracle RAC database. For example, `-force` (to override any warnings), `-debug` (to view more debug information), and `-invPtrLoc <Location>` (for UNIX only). Ensure that the parameters are separated by white space.

You can also specify OCFS devices in the Installer Parameters field in the following format, separating devices with commas:

Device Number:Partition Number: Drive letter: [DATA | SOFTWARE]

For example:

Additional Parameters	
* Working Directory	/tmp
Installer Parameters	-ocfs_devices=1:1:E:DATA,1:2:F:DATA

Click **Next**. You will come back to the Configure page. If you have configured the source and destination location for the software, the Configure Software task will have a Configured status.

9. Click on the Create Databases link.
10. In the Database Template page, choose the database template location. The location can be Software Library or Oracle home. The template selected must be compatible with the selected Oracle home version.

If you have selected **Software Library**, click on the search icon and select the template from the Software Library. Specify **Temporary Storage Location on Managed Host(s)**. This location must be present on the reference node that you selected earlier.

Click **Show Template Details** to view details of the selected template. You can view initialization parameters, table spaces, data files, redo log groups, common options, and other details of the template.

If you have selected **Oracle Home**, select the template from the Oracle home. The default location is `ORACLE_HOME/assistants/dbca/templates`.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

11. In the Identification and Placement page, select the Oracle RAC database configuration type, whether Policy Managed or Admin Managed.

For admin-managed database, select nodes on which you want to create the cluster database.

For policy-managed database, select the server pools to be used for creating the database, from the list of existing server pools, or choose to create a new server pool. Policy-managed databases can be created for database versions 11.2 and higher. For database versions lower than 11.2, you will need to select nodes to create the Oracle RAC database.

Specify **Global Database Name** and **SID** prefix. Specify the **Database Credentials** for SYS, SYSTEM, and DBSNMP. You can choose to specify the same or different passwords for each of these user accounts.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

12. In the Storage Locations page, select the storage type for Oracle RAC Database as **File System**.

In the Database Files Location section, specify the location where data files, temporary files, redo logs, and control files will be stored. These locations must be on shared storage such as cluster file system location or ASM diskgroups.

- Select **Use Database File Locations from Template** to select defaults from the template used.
- Select **Use Common Location for All Database Files** to specify a different location.

If you select **Use Oracle Managed Files (OMF)**, in the Multiplex Redo Logs and Control Files section, you can specify locations to store duplicate copies of redo logs and control files. Multiplexing provides greater fault-tolerance. You can specify upto five locations.

In the Recovery Files Location section, select **Use same storage type as database files location** to use the same storage type for recovery files as database files. Select **Use Flash Recovery Area** and specify the location for recovery-related files and Fast Recovery Area Size.

Select **Enable Archiving** to enable archive logging. Click **Specify Archive Log Locations** and specify upto nine archive log locations. If the log location is not specified, the logs will be saved in the default location.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

13. In the Initialization Parameters page, select the memory management type as **Automatic Memory Management** or **Automatic Shared Memory Management**. Select **Specify Memory Settings as Percentage of Available Memory** to specify memory settings as percentage of available physical memory. For Automatic Shared Memory management, specify **Total SGA** and **Total PGA**. For Automatic Memory Management, specify **Total Memory for Oracle**.

In the Database sizing section, specify the **Block Size** and number of **Processes**. If you have selected a database template with datafiles in the Database Template page, you cannot edit the Block Size.

Specify the Host CPU Count. The maximum CPU count that can be specified is equal to the number of CPUs present on the host.

In the Character Sets section, select the default character set. The default character set is based on the locale and operating system.

Select a national character set. The default is **AL16UTF16**.

In the Database Connection Mode section, select the dedicated server mode. For shared server mode, specify the number of shared servers.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

14. In the Additional Configuration Options page, select custom scripts from the Software Library or your local disk. If you have selected a Structure Only database template in the Database Template page, you can also view and edit database options.

Click on the Lock icon to lock the field. Click **Next**.

15. Review the information you have provided and click **Next**. You will come back to the Configure page. If you have configured the database, the Create Databases task will have a Configured status. Click **Next**.

16. Click the Compliance Standards link.

17. In the Configuration Standards Target Association page, select a Compliance Standard to be associated with the database. Click **Next**.

18. In the Configure page, click **Next**.

19. The Custom Properties page will be displayed only for user customized deployment procedures that require custom parameters. Specify custom properties for the deployment, if any. Click **Next**.

20. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure to allow me to analyze results after performing prerequisite checks** to pause the procedure execution after all prerequisite checks are performed.

Click **Next**.

21. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment.

22. In the Operator role, launch the saved deployment procedure. Add targets for provisioning and provide values for configurable fields in the deployment procedure.

23. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the Status link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

24. After the procedure execution is completed, click on the **Targets** menu and select **All Targets** to navigate to the All Targets page and verify that the newly provisioned databases appear as Cloud Control targets.

Note: if the Deployment Procedure fails, then review log files described in [Section E.8](#).

7.5 Provisioning Oracle Real Application Clusters Database with File System on a New Cluster

This section covers the following:

- [Prerequisites](#)
- [Procedure](#)

7.5.1 Prerequisites

Before running the Deployment Procedure, meet the prerequisites listed in [Section 4.3](#).

7.5.2 Procedure

To provision Oracle RAC databases on a new cluster, follow these steps:

1. Log in as a designer, and from the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the **Provision Oracle RAC Database** Deployment Procedure and click **Launch**. The Oracle RAC Database provisioning wizard is launched.
3. In the Select Hosts page, select the provisioning and configuration actions and destination hosts.

If you want to use a provisioning profile for the deployment, choose **Select a Provisioning Profile** and then select the profile with previously saved configuration parameters.

In the Select Tasks to Perform section, do the following:

- Select **Deploy Grid Infrastructure** to provision Grid Infrastructure
- Select **Deploy Database software** to provision Oracle RAC databases
- Select **Configure Grid Infrastructure** to add configure Grid Infrastructure
- Select **Create a New Database** to create and configure the database



In the Select destination hosts section, click **Add** to select the destination host where you want to deploy and configure the Grid Infrastructure and database.

Click on the Lock icon against the fields that you do not want to be edited in the operator role. For more information about the lock down feature in deployment procedures, see [Section 4.1](#).

Click **Next**.

4. In the Configure page, click on the Setup Hosts link.
5. In the Specify OS Users page, specify the operating system users and groups required to provision the database.

For Database User and ASM User, select the Normal User and Privileged User to be added to the OS group.

Click **Next**.

6. In the Specify OS Groups page, specify the OS Groups to use for operating system authentication. Ensure that the groups corresponding to the following roles already exist on the hosts you select for provisioning.
 - Inventory Group (OINSTALL)
 - ASM Database Administrator (ASMDBA)
 - ASM Instance Operator (ASMOPER)
 - Database Administrator (OSDBA)
 - Database Operator (OSOPER)
 - ASM Instance Administrator (OSASM)

Click **Next**. You will come back to the Configure page. If you have configured the destination hosts, the Setup Hosts task will have a Configured status.

7. Click on the Deploy Software link.
8. In the Select Software Locations page, specify the locations where the software binaries of Oracle Grid Infrastructure and Oracle RAC can be placed, that is, the \$ORACLE_HOME location. As a designer, you can click on the Lock icon to lock these fields. These fields will then not be available for editing in the operator role.

In the Source section, select the Software Library location for the **Grid Infrastructure** and **Oracle Database** binaries.

In the Destination location, specify the following:

- **Oracle Base for Grid Infrastructure**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the Grid Infrastructure can be stored.
- **Grid Infrastructure Home**, a location on the destination host where the Grid Infrastructure software can be provisioned. This is the Oracle home directory for Grid Infrastructure. Do not select a location that is a subdirectory of the Oracle Base for Grid Infrastructure or database. Select **Shared Grid Infrastructure home** to enable Grid Infrastructure Oracle Home on shared locations. Ensure that the directory path you provide meets the requirements described in [Section 7.3.2.1](#).
- **Oracle Base for Database**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the database can be stored. This location is used for storing only the dump files and is different from the Oracle home directory where the database software will be installed.

- **Database Oracle Home**, a location on the destination host where the database software can be provisioned. This is the Oracle home directory for the database. Select **Shared Database Oracle home** to enable Database Oracle Home on shared locations.

For Grid Infrastructure, Oracle Base is `/u01/app/user` and Oracle Home is `%ORACLE_BASE/../../grid`. You can use `%ORACLE_BASE%` and `%GI_ORACLE_BASE%` to specify the relative paths which will be interpolated to their respective values.

In the Additional Parameters section, specify the **Working Directory** on the destination host where the files related to cloning can be staged temporarily. Ensure that you have approximately 7 GB of space for this directory. For **Installer Parameters**, specify any additional Oracle Universal Installer (OUI) parameters you want to run while provisioning Oracle Grid Infrastructure. For example, `-force` (to override any warnings), `-debug` (to view more debug information), and `-invPtrLoc <Location>` (for UNIX only). Ensure that the parameters are separated by white space.

You can also specify OCFS devices in the Installer Parameters field in the following format, separating devices with commas:

Device Number:Partition Number: Drive letter: [DATA | SOFTWARE]

For example:

Additional Parameters	
* Working Directory	/tmp
Installer Parameters	-ocfs_devices=1:1:E:DATA,1:2:F:DATA

Click **Next**. You will come back to the Configure page. If you have configured the source and destination location for the software, the Configure Software task will have a Configured status.

9. Click on the Configure Grid Infrastructure link.
10. In the Select Storage page, select the storage type for Grid Infrastructure as **Automatic Storage Management** and database as **File System** to indicate the storage type for storing voting disk and Oracle Cluster Registry (OCR). Voting disk and OCR are used by Oracle Clusterware to manage its resources.

As a designer, you can click on the Lock icon to lock these fields. These fields will then not be available for editing in the operator role.

Click **Next**.

11. In the Configure GI page, in the Basic Settings section, specify the **Cluster Name**, **SCAN Name**, and **SCAN Port**. The default SCAN port is port 1521, but you can specify another port of your choice. The deployment procedure verifies that the SCAN port provided is a valid port number, and is not used for any other purpose. After installation, a TNS listener listens to this port to respond to client connections to the SCAN name.

Configure Grid Infrastructure **Select Storage** **Configure GI** Configure Grid Infrastructure

Provision Oracle RAC Database : Configure GI

Basic Settings

Cluster Name: crs1

SCAN Name: crs1-scan

SCAN Port: 1521

GNS Settings

Configure GNS

GNS Sub System:

GNS VIP Address:

GI Network

+ Add - Delete...

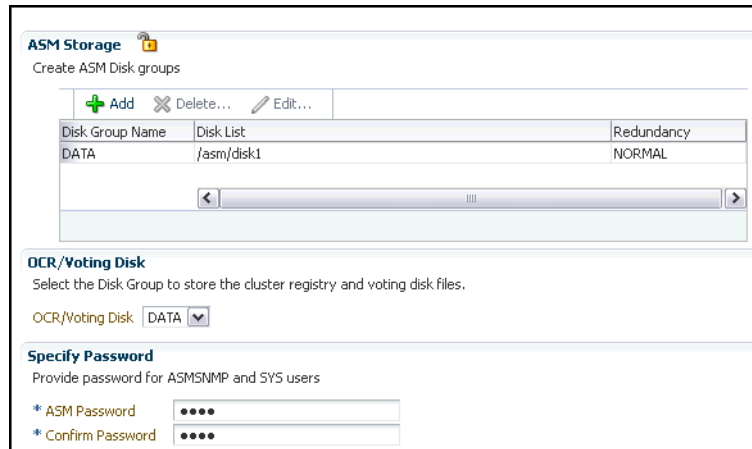
Interface Name	Interface Subnet	Usage
eth0	140.84.128.0	PUBLIC

In the GNS Settings section, select **Configure GNS** and specify the **GNS Sub System** and **GNS VIP Address** if you want virtual host names outside the cluster to have dynamically assigned names.

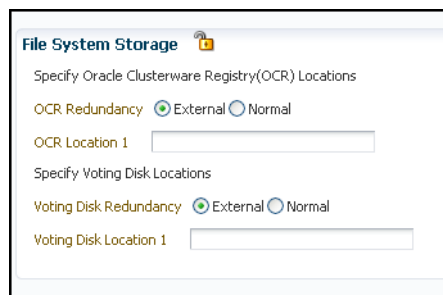
In the GI Network section, by default, the network interfaces that have the same name and subnet for the selected destination hosts are automatically detected and displayed. Validate these network interface configuration details. From the Usage column, select **Public** to configure the interface as public interface, or **Private** to configure the interface as private interface.

Click **Add** to add an interface and specify the **Interface Name** and **Interface Subnet** and click **OK**. Select the Usage as **Public**, **Private**, or **Do Not Use** if you do not want to use the interface.

If you have chosen storage type as Automatic Storage Management for Grid Infrastructure, in the ASM Storage section, select from the ASM Disk Groups that have been discovered by Cloud Control and are displayed in the table. Click **Add** to add an ASM Disk Group. In the Add/Edit Disk Group dialog box, specify the **Disk Group Name**, **Disk List**, and specify the redundancy as **Normal**, **High**, or **External**. Click **OK**. Select the OCR/Voting Disk to store cluster registry and voting disk files, and specify the ASM credentials for ASMSNMP and SYS users.



If you have chosen storage type as File System for Oracle RAC database, in the File System Storage section, specify the storage location for Oracle Cluster Registry (OCR) and voting disks. Select Normal or External to indicate the redundancy level, and specify their locations.



As a designer, you can click on the Lock icon to lock these fields. These fields will then not be available for editing in the operator role.

Click **Next**. You will come back to the Configure page. If you have configured the storage options for the Grid Infrastructure and database, the Configure Grid Infrastructure task will have a completed status.

12. Click on the Create Databases link.
13. In the Database Template page, choose the database template location. The location can be Software Library or Oracle home. The template selected must be compatible with the selected Oracle home version.

If you have selected **Software Library**, click on the search icon and select the template from the Software Library. Specify **Temporary Storage Location on Managed Host(s)**. This location must be present on the reference node that you selected earlier.

Click **Show Template Details** to view details of the selected template. You can view initialization parameters, table spaces, data files, redo log groups, common options, and other details of the template.

If you have selected **Oracle Home**, select the template from the Oracle home. The default location is ORACLE_HOME/assistants/dbca/templates.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

14. In the Identification and Placement page, select the Oracle RAC database configuration type, whether Policy Managed or Admin Managed.

For admin-managed database, select nodes on which you want to create the cluster database.

For policy-managed database, select the server pools to be used for creating the database, from the list of existing server pools, or choose to create a new server pool. Policy-managed databases can be created for database versions 11.2 and higher. For database versions lower than 11.2, you will need to select nodes to create the Oracle RAC database.

Specify **Global Database Name** and **SID** prefix. Specify the **Database Credentials** for SYS, SYSTEM, and DBSNMP. You can choose to specify the same or different passwords for each of these user accounts.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

15. In the Storage Locations page, select the storage type for Oracle RAC Database as **File System**.

In the Database Files Location section, specify the location where data files, temporary files, redo logs, and control files will be stored. These locations must be on shared storage such as cluster file system location or ASM diskgroups.

- Select **Use Database File Locations from Template** to select defaults from the template used.
- Select **Use Common Location for All Database Files** to specify a different location.

If you select **Use Oracle Managed Files (OMF)**, in the Multiplex Redo Logs and Control Files section, you can specify locations to store duplicate copies of redo logs and control files. Multiplexing provides greater fault-tolerance. You can specify upto five locations.

In the Recovery Files Location section, select **Use same storage type as database files location** to use the same storage type for recovery files as database files. Select **Use Flash Recovery Area** and specify the location for recovery-related files and Fast Recovery Area Size.

Select **Enable Archiving** to enable archive logging. Click **Specify Archive Log Locations** and specify upto nine archive log locations. If the log location is not specified, the logs will be saved in the default location.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

16. In the Initialization Parameters page, select the memory management type as **Automatic Memory Management** or **Automatic Shared Memory Management**. Select **Specify Memory Settings as Percentage of Available Memory** to specify memory settings as percentage of available physical memory. For Automatic Shared Memory management, specify **Total SGA** and **Total PGA**. For Automatic Memory Management, specify **Total Memory for Oracle**.

In the Database sizing section, specify the **Block Size** and number of **Processes**. If you have selected a database template with datafiles in the Database Template page, you cannot edit the Block Size.

Specify the Host CPU Count. The maximum CPU count that can be specified is equal to the number of CPUs present on the host.

In the Character Sets section, select the default character set. The default character set is based on the locale and operating system.

Select a national character set. The default is **AL16UTF16**.

In the Database Connection Mode section, select the dedicated server mode. For shared server mode, specify the number of shared servers.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

17. In the Additional Configuration Options page, select custom scripts from the Software Library or your local disk. If you have selected a Structure Only database template in the Database Template page, you can also view and edit database options.

Click on the Lock icon to lock the field. Click **Next**.

18. Review the information you have provided and click **Next**. You will come back to the Configure page. If you have configured the database, the Create Databases task will have a Configured status. Click **Next**.

19. Click the Compliance Standards link.

20. In the Configuration Standards Target Association page, select a Compliance Standard to be associated with the database. Click **Next**.

21. In the Configure page, click **Next**.

22. The Custom Properties page will be displayed only for user customized deployment procedures that require custom parameters. Specify custom properties for the deployment, if any. Click **Next**.

23. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure to allow me to analyze results after performing prerequisite checks** to pause the procedure execution after all prerequisite checks are performed.

Click **Next**.

24. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment.

25. In the Operator role, launch the saved deployment procedure. Add targets for provisioning and provide values for configurable fields in the deployment procedure.

26. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the Status link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.
27. After the procedure execution is completed, click on the **Targets** menu and select **All Targets** to navigate to the All Targets page and verify that the newly provisioned databases appear as Cloud Control targets.

Note: if the Deployment Procedure fails, then review log files described in [Section E.8](#).

Provisioning Oracle Real Application Clusters One (Oracle RAC One) Node Databases

This chapter explains how you can provision Oracle Real Application Clusters One (Oracle RAC One) node databases using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Getting Started](#)
- [Deployment Procedures](#)
- [Provisioning Oracle Real Application Clusters One Node Databases](#)

8.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in provisioning Oracle RAC One node databases. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision Oracle RAC One node. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 8–1 *Getting Started with Provisioning Oracle RAC One Node Databases*

Step	Description	Reference Links
Step 1	<p>Understanding the Deployment Procedures</p> <p>To provision Oracle RAC One node databases, you will need to run two deployment procedures.</p>	<ul style="list-style-type: none"> ▪ To learn about the deployment procedures to run for provisioning Oracle RAC One node databases, see Section 8.2.
Step 2	<p>Understanding the Usecase</p> <p>This section lists the usecase to provision Oracle RAC One node databases.</p>	<ul style="list-style-type: none"> ▪ To understand the usecase for provisioning Oracle RAC One node databases, see Section 8.3.
Step 3	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	<ul style="list-style-type: none"> ▪ To learn about the prerequisites for provisioning Oracle RAC One node databases, see Section 8.3.1.

Table 8–1 (Cont.) Getting Started with Provisioning Oracle RAC One Node Databases

Step	Description	Reference Links
Step 4	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully provision Oracle RAC One node databases.</p>	<ul style="list-style-type: none"> To provision Oracle RAC One node databases, follow the steps explained in Section 8.3.2.

8.2 Deployment Procedures

To provision Oracle RAC one database using Cloud Control, use the following Deployment Procedures:

- *Provision Oracle RAC Database + Create Oracle Database*

Use the Provision Oracle RAC Database deployment procedure to provision Oracle RAC database software and then run the Create Oracle Database deployment procedure to create Oracle RAC One databases.

8.3 Provisioning Oracle Real Application Clusters One Node Databases

This section describes how you can provision Oracle RAC one Node databases.

This section covers the following:

- [Prerequisites](#)
- [Procedure](#)

8.3.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

Following are the infrastructure-related prerequisites to be met by the administrator who creates the infrastructure for provisioning deployment procedures:

- Ensure that you meet the infrastructure requirements described in [Chapter 2](#).
- Meet the hardware, software, and network requirements for Oracle Grid Infrastructure and Oracle RAC installation on the target hosts. For information about the hardware, software, and network requirements for Oracle Grid Infrastructure and Oracle RAC installation, refer to the Oracle Grid Infrastructure Installation Guide 11g Release 2 (11.2).
- Discover and monitor the destination hosts in Cloud Control. For this purpose, you need the latest version of Oracle Management Agent (Management Agent) on the destination hosts. For more information refer to the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. Ensure that the agents are installed in the same location on all hosts.
- Set up the Oracle Software Library (Software Library). Ensure that the installation media, database templates, or provisioning entities are available in the Software Library. For information about creating them, see [Section 4.3](#). Alternatively, use a provisioning profile to store the database template. For information about creating a database provisioning profile, see [Section 4.3.5](#).

- Store the operating system credentials of the destination hosts as preferred credentials in Oracle Management Repository (Management Repository) or use Named Credentials.

If you are using SUDO, PowerBroker, see [Section 2.3.3](#) for information on setting up these authentication utilities.

- The user configuring the deployment procedure will need to be a member of the groups specified below. If these groups do not exist, then the Deployment Procedure automatically creates them. However, if these have to be created on NIS, then you must create them manually before running the Deployment Procedure. For information about creating these operating system groups, refer to the Oracle Grid Infrastructure Installation Guide 11g Release 2 (11.2).

The Oracle Database user (typically *oracle*) must be a member of the following groups:

- Inventory Group (OINSTALL) as the primary group
- Database Administrator (OSDBA)
- Database Operator (OSOPER)

The Grid Infrastructure user (typically *grid*) must be a member of the following groups:

- Inventory Group (OINSTALL) as the primary group
- ASM Database Administrator (ASMDBA)
- ASM Instance Operator (ASMOPER)
- ASM Instance Administrator (OSASM)

The Oracle RAC Database user must be a member of the following group:

- ASM Database Administrator (ASMDBA)

- Ensure that you use an operating system user that has write permission on the following locations:
 - Oracle base directory for Grid Infrastructure where diagnostic data files related to Grid Infrastructure can be stored.
 - Oracle base directory for database where diagnostic data files related to database can be stored.
 - Grid Infrastructure software directory where Grid Infrastructure software can be provisioned.
 - Database software location where database software can be provisioned
 - Working directory where cloning-related files can be staged.
- Ensure that you have `Operator-Any Target` privileges in Cloud Control.

Prerequisites for Operators

Following are the deployment procedure-related prerequisites to be met by the operator who runs the provisioning deployment procedures:

- Ensure that as an operator, you have permissions to view credentials (set and locked by the designer), view targets, submit jobs, and launch deployment procedures.

- Ensure that the operating system groups you specify for the following groups already exist on the hosts you select for provisioning. The operating system users of these groups automatically get the respective privileges.
 - Inventory Group (OINSTALL)
 - ASM Database Administrator (ASMDBA)
 - ASM Instance Operator (ASMOPER)
 - Database Administrator (OSDBA)
 - Database Operator (OSOPER)
 - ASM Instance Administrator (OSASM)
- Ensure that you have `Operator-Any Target` privileges in Cloud Control.

8.3.2 Procedure

To provision Oracle RAC One node database, follow these steps:

1. Log in as a designer, and from the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the Provision Oracle RAC Database Deployment Procedure and click **Launch**. The Oracle RAC Database provisioning wizard is launched.
3. In the Select Hosts page, select the provisioning and configuration actions and destination hosts.

If you want to use a provisioning profile for the deployment, choose **Select a Provisioning Profile** and then select the profile with previously saved configuration parameters.

In the Select Tasks to Perform section, do the following:

- Select **Deploy Grid Infrastructure** to provision Grid Infrastructure
- Select **Deploy Database software** to provision Oracle RAC databases
- Select **Configure Grid Infrastructure** to add configure Grid Infrastructure

In the Select destination hosts section, click **Add** to select the destination host where you want to deploy and configure the Grid Infrastructure and database.

Click **Next**.

4. In the Configure page, click on the Setup Hosts link.
5. In the Specify OS Users page, specify the operating system users and groups required to provision the database.

For Database User and ASM User, select the Normal User and Privileged User to be added to the OS group.

Click **Next**.

6. In the Specify OS Groups page, specify the OS Groups to use for operating system authentication. Ensure that these groups already exist on the hosts you select for provisioning.
 - Inventory Group (OINSTALL)
 - ASM Database Administrator (ASMDBA)
 - ASM Instance Operator (ASMOPER)

- Database Administrator (OSDBA)
- Database Operator (OSOPER)
- ASM Instance Administrator (OSASM)

Click **Next**. You will come back to the Configure page. If you have configured the destination hosts, the Setup Hosts task will have a Configured status.

7. Click on the Deploy Software link.
8. In the Select Software Locations page, specify the locations where the software binaries of Oracle Grid Infrastructure and Oracle RAC can be placed, that is, the \$ORACLE_HOME location. As a designer, you can click on the Lock icon to lock these fields. These fields will then not be available for editing in the operator role.

In the Source section, select the Software Library location for the **Grid Infrastructure** and **Oracle Database** binaries.

In the Destination location, specify the following:

- **Oracle Base for Grid Infrastructure**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the Grid Infrastructure can be stored.
- **Grid Infrastructure Home**, a location on the destination host where the Grid Infrastructure software can be provisioned. This is the Oracle home directory for Grid Infrastructure. Do not select a location that is a subdirectory of the Oracle Base for Grid Infrastructure or database. Select **Shared Grid Infrastructure home** to enable Grid Infrastructure Oracle Home on shared locations. Ensure that the directory path you provide meets the requirements described in [Section 7.3.2.1](#).
- **Oracle Base for Database**, a location on the destination host where the diagnostic and administrative logs, and other logs associated with the database can be stored. This location is used for storing only the dump files and is different from the Oracle home directory where the database software will be installed.
- **Database Oracle Home**, a location on the destination host where the database software can be provisioned. This is the Oracle home directory for the database. Select **Shared Database Oracle home** to enable Database Oracle Home on shared locations.

In the Additional Parameters section, specify the **Working Directory** on the destination host where the files related to cloning can be staged temporarily. Ensure that you have approximately 7 GB of space for this directory. For **Installer Parameters**, specify any additional Oracle Universal Installer (OUI) parameters you want to run while provisioning Oracle Grid Infrastructure. For example, `-force` (to override any warnings), `-debug` (to view more debug information), and `-invPtrLoc <Location>` (for UNIX only). Ensure that the parameters are separated by white space.

Click **Next**. You will come back to the Configure page. If you have configured the source and destination location for the software, the Configure Software task will have a Configured status.

9. Click on the Configure Grid Infrastructure link.
10. In the Select Storage page, select the storage type for Grid Infrastructure and database as **Automatic Storage Management** or **File System** to indicate the storage type for storing voting disk and Oracle Cluster Registry (OCR). Voting

disk and OCR are used by Oracle Clusterware to manage its resources. You can choose from the following options:

- Automatic Storage Management for both Grid Infrastructure and Oracle RAC Database
- Automatic Storage Management for Grid Infrastructure and File System for Oracle RAC Database
- File System for both Grid Infrastructure and Oracle RAC Database
- File System for Grid Infrastructure and Automatic Storage Management for Oracle RAC Database

As a designer, you can click on the Lock icon to lock these fields. These fields will then not be available for editing in the operator role.

Click **Next**.

11. In the Configure GI page, in the Basic Settings section, specify the **Cluster Name**, **SCAN Name**, and **SCAN Port**. The default SCAN port is port 1521, but you can specify another port of your choice. The deployment procedure verifies that the SCAN port provided is a valid port number, and is not used for any other purpose. After installation, a TNS listener listens to this port to respond to client connections to the SCAN name.

In the GNS Settings section, select **Configure GNS and auto-assign with DHCP** and specify the **GNS Sub System** and **GNS VIP Address** if you want virtual host names outside the cluster to have dynamically assigned names.

In the GI Network section, by default, the network interfaces that have the same name and subnet for the selected destination hosts are automatically detected and displayed. Validate these network interface configuration details. From the Usage column, select **Public** to configure the interface as public interface, or **Private** to configure the interface as private interface.

Click **Add** to add an interface and specify the **Interface Name** and **Interface Subnet** and click **OK**. Select the Usage as **Public**, **Private**, or **Do Not Use** if you do not want to use the interface.

If you have chosen storage type as Automatic Storage Management for either or both Grid Infrastructure and Oracle RAC Database, in the ASM Storage section, select from the ASM Disk Groups that have been discovered by Cloud Control and are displayed in the table. Click **Add** to add an ASM Disk Group. In the Add/Edit Disk Group dialog box, specify the **Disk Group Name**, **Disk List**, and specify the redundancy as **Normal**, **High**, or **External**. Click **OK**. Select the OCR/Voting Disk to store cluster registry and voting disk files, and specify the ASM credentials for ASMSNMP and SYS users.

If you have chosen storage type as File System for Grid Infrastructure or Oracle RAC database, in the File System Storage section, specify the storage location for Oracle Cluster Registry (OCR) and voting disks. Select **Normal** or **External** to indicate the redundancy level, and specify their locations.

As a designer, you can click on the Lock icon to lock these fields. These fields will then not be available for editing in the operator role.

Click **Next**. You will come back to the Configure page. If you have configured the storage options for the Grid Infrastructure and database, the Configure Grid Infrastructure task will have a completed status. Click **Next**.

12. The Custom Properties page will be displayed only for user customized deployment procedures that require custom parameters. Specify custom properties for the deployment, if any. Click **Next**.
13. In the Schedule page, if you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. Click **Next**.
14. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment.
15. In the Database Procedures page, select the Create Oracle Database Deployment Procedure and click **Launch**. The Create Oracle Database provisioning wizard is launched.
16. In the Database Version and Type page, select the database **Version** and select **Oracle RAC One Node Database**.

In the Cluster section, select the cluster and Oracle Home provisioned earlier. Select a reference host to perform validations to use as reference to create database on the cluster.

Select **Cluster Credentials** or add new. Click the plus icon to add new credentials and specify **User Name**, **Password**, and **Run Privileges** and save the credentials.

Click **Next**.

17. In the Database Template page, choose the database template location. The location can be Software Library or Oracle home. The template selected must be compatible with the selected Oracle home version.

If you have selected **Software Library**, click on the search icon and select the template from the Software Library. Specify **Temporary Storage Location on Managed Host(s)**. This location must be present on the reference node that you selected earlier.

Click **Show Template Details** to view details of the selected template. You can view initialization parameters, table spaces, data files, redo log groups, common options, and other details of the template.

If you have selected **Oracle Home**, select the template from the Oracle home. The default location is ORACLE_HOME/assistants/dbca/templates.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

18. In the Identification and Placement page, select nodes on which you want to create the cluster database. Specify **Global Database Name** and **SID** prefix. Specify the **Database Credentials** for SYS, SYSTEM, and DBSNMP. Select the type of Oracle RAC database, whether Policy Managed or Admin Managed. Specify the **Service Name**.

Note: Database Service Name is used by applications to connect to the Oracle RAC One Node database and to facilitate online relocation.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

19. In the Storage Locations page, select the storage type, whether File System or Automatic Storage Management (ASM).

In the Database Files Location section, specify the location where data files, temporary files, redo logs, and control files will be stored.

- Select **Use Database File Locations from Template** to select defaults from the template used.
- Select **Use Common Location for All Database Files** to specify a different location.

If you select **Use Oracle Managed Files (OMF)**, in the Multiplex Redo Logs and Control Files section, you can specify locations to store duplicate copies of redo logs and control files. Multiplexing provides greater fault-tolerance. You can specify upto five locations.

In the Recovery Files Location section, select **Use Flash Recovery Area** and specify the location for recovery-related files and Fast Recovery Area Size.

In the Archive Log Settings section, select **Enable Archiving** to enable archive logging. In the Specify Archive Log Locations, you can specify upto nine archive log locations. If the log location is not specified, the logs will be saved in the default location.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

20. In the Initialization Parameters page, select the memory management type as **Automatic Memory Management** or **Automatic Shared Memory Management**. Select **Specify Memory Settings as Percentage of Available Memory** to specify memory settings as percentage of available physical memory. For Automatic Shared Memory management, specify **Total SGA** and **Total PGA**. For Automatic Memory Management, specify **Total Memory for Oracle**.

In the Database sizing section, specify the **Block Size** and number of **Processes**. If you have selected a database template with datafiles in the Database Template page, you cannot edit the Block Size.

Specify the Host CPU Count. The maximum CPU count that can be specified is equal to the number of CPUs present on the host.

In the Character Sets section, select the default character set. The default character set is based on the locale and operating system.

Select a national character set. The default is **AL16UTF16**.

In the Database Connection Mode section, select the dedicated server mode. For shared server mode, specify the number of shared servers.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

21. In the Additional Configuration Options page, select custom scripts from the Software Library. If you have selected a Structure Only database template in the

Database Template page, you can also view and edit database options. Click on the Lock icon to lock the field. Click **Next**.

- 22.** In the Schedule page, specify a Deployment Procedure Instance Name and a schedule for the deployment. If you want to run the procedure immediately, then retain the default selection, that is Immediately. If you want to run the procedure later, then select Later and provide time zone, start date, and start time details. Click **Next**.
- 23.** In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment.
- 24.** In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the Status link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

Provisioning Oracle Real Application Clusters for 10g and 11g

This chapter explains how you can provision Oracle Real Application Clusters (Oracle RAC) for 10g and 11g Release 1 using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Getting Started](#)
- [Core Components Deployed](#)
- [Cloning a Running Oracle Real Application Clusters](#)
- [Provisioning Oracle Real Application Clusters Using Gold Image](#)
- [Provisioning Oracle Real Application Clusters Using Archived Software Binaries](#)

9.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in provisioning Oracle RAC for 10g and 11g Release 1. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision Oracle RAC for 10g and 11g Release 1. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 9–1 *Getting Started with Provisioning Oracle RAC*

Step	Description	Reference Links
Step 1	<p>Understanding the Components Provisioned</p> <p>Understand the core components provisioned.</p>	To learn about the core components that are provisioned, see Section 9.2 .
Step 2	<p>Selecting the Use Case</p> <p>This chapter covers a few use cases for provisioning Oracle RAC. Select the use case that best matches your requirement.</p>	<ul style="list-style-type: none"> ■ To learn about cloning an existing Oracle RAC, see Section 9.3. ■ To learn about provisioning Oracle RAC using a gold image, see Section 9.4. ■ To learn about provisioning Oracle RAC using the software binaries from an installation medium, see Section 9.5.

Table 9–1 (Cont.) Getting Started with Provisioning Oracle RAC

Step	Description	Reference Links
Step 3	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	<ul style="list-style-type: none"> ■ To learn about prerequisites for cloning an existing Oracle RAC, see Section 9.3.1. ■ To learn about the prerequisites for provisioning Oracle RAC using a gold image, see Section 9.4.1. ■ To learn about the prerequisites for provisioning Oracle RAC using the software binaries from an installation medium, see Section 9.5.1.
Step 4	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully provision Oracle RAC.</p>	<ul style="list-style-type: none"> ■ To clone an existing Oracle RAC, follow the steps explained in Section 9.3.2. ■ To provision Oracle RAC using a gold image, follow the steps explained in Section 9.4.2. ■ To provision Oracle RAC using the software binaries from an installation medium, follow the steps explained in Section 9.5.2.

9.2 Core Components Deployed

When you provision Oracle RAC, essentially, the Deployment Procedures deploy the following core components:

- Oracle Clusterware
- Oracle RAC Database
- Optionally, Automatic Storage Management (ASM)

You can deploy ASM either in the same Oracle home as the one for Oracle RAC Database, or in a completely different Oracle home (recommended).

Note: When you run the Deployment Procedures to provision Oracle RAC on a shared file system, the software binaries are installed in the shared location, but the configuration happens on all nodes. To configure new nodes, run the *One Click Extend Cluster Database* procedure to extend the Oracle RAC stack to other nodes.

9.3 Cloning a Running Oracle Real Application Clusters

This section describes how you can clone an existing Oracle RAC installation that is running on a host monitored by Cloud Control.

This section covers the following:

- [Prerequisites](#)
- [Cloning Procedure](#)

9.3.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites.

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- If you want to clone Oracle RAC 11g Release 1 (11.1.0.6) on Solaris platforms, then apply patch# 6486988 on the Oracle home that needs to be cloned.
- Ensure that the target hosts have the necessary hardware and software required for Oracle RAC. The hardware requirements include setting up of the following:
 - Private Network: The network interface cards must be installed on each node and connected to each other.
 - Shared Storage Between Nodes: The shared storage is required for OCR, Voting disks and the data files.
- Ensure that the Virtual IPs are set up in the DNS. If you choose to set up the Virtual IPs locally, then the IP addresses can be specified using the Deployment Procedure, and the procedure will set them up for you.
- If you want to use a custom template to create a structure for the database, then create a template (a .dbt file), and store it in a location accessible from the target hosts. The file may be on the target host or on a shared location. For information about creating templates, see [Section 4.3.7, "Creating Database Templates"](#).
- Ensure that operating system users such as *oracle* and *crsuser* are available on all nodes of the cluster. These users must be a part of the relevant operating system groups such as *dba* and *oinstall*.

For more information, see Oracle Clusterware Installation Guide available at:

<http://www.oracle.com/pls/db111/homepage>

- Ensure that the User IDs for operating system users and the Group IDs for operating system groups are identical on all nodes of the cluster.

Prerequisites for Operators

- Ensure that you do NOT use an NIS-based operating system user.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure and its commands on the target hosts. If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges. For information about customization, see [Chapter 33](#).
- Compare the configuration of the source and target hosts and ensure that they have the same configuration. If the configurations are different, then contact your system administrator and fix the inconsistencies before running the Deployment Procedure.

To compare the configuration of the hosts, in Cloud Control, click **Targets** and then **Hosts**. On the Hosts page, click the name of the source host to access its Home page, and then from the Host menu, click **Configuration** and then click **Compare**.

- While selecting the source, remember to remove `sqlnet.ora` from the list of files mentioned in **Files to Exclude**.
- Ensure that the `umask` value on the target host is 022.

9.3.2 Cloning Procedure

To clone an existing Oracle RAC installation, follow these steps:

1. From the Enterprise menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Provisioning page, select one of the following, and click **Launch**.
 - a. To run the Deployment Procedure on UNIX platforms, Select **Provision Oracle Clusterware / RAC for UNIX and RDBMS versions 10g/11g**.
 - b. To run the Deployment Procedure on Microsoft Windows platforms, select **Provision Oracle Clusterware / RAC for Windows and RDBMS versions 10g/11g**.

Cloud Control displays the Select Source page of the Deployment Procedure.

3. On the Select Source page, do the following:
 - a. In the Select Source section, select **Select from Existing Installations**. Then click the torch icon for **Reference Host** and select the host on which the existing Oracle RAC installation is running. Once you select the reference host, the application automatically displays the working directory and the details of the selected Oracle Clusterware and Oracle Database.

If you want to save the selected Oracle Clusterware and Oracle Database as gold images in the Software Library, then click **Save to Software Library**. Oracle Clusterware is saved as a *Clusterware Clone* component type and Oracle Database is stored as a *Database Clone* component type, respectively.

Note:

- Maintain different locations as working directories in case a shared disk is used between the source host and the destination host.
 - `sqlnet.ora` hardcodes Oracle base from source install. If you do not remove the file, Oracle tools and utilities will use an incorrect Oracle base and an error message stating that the current location is not writable is displayed.
-
-

- b. Click **Next**.
4. On the Select Hosts page, do the following:
 - a. In the Hosts to Include in Cluster section, click **Add** and select the target hosts that should form the cluster. To see more details about the selected hosts, click **Show Options**.

Note: When you click **Add**, the Select Target pop-up window appears. On this page, by default, the **Show Suitable Hosts** option is selected and the table lists only those hosts that are best suited for provisioning. If you do not find the host you want to add, then select **Show All Hosts** to view a complete list of hosts.

By default, Private Host Name and Virtual Host Name are automatically prefilled with values. Edit them and specify values that match with your environment. Optionally, you can also specify their IP addresses.

Note: If the prefilled, default values of Private Host Name and Virtual Host Name are incorrect, then see the workaround described in [Appendix E, "Troubleshooting Issues"](#).

If you already have these details stored in cluster configuration file, then click **Import From File** to select that cluster configuration file. This file typically contains information about the new hosts to be added. To understand how a cluster configuration file looks, see the sample file shown in [Section 9.5.2.1, "Sample Cluster Configuration File"](#).

To configure the private and public network interfaces, click **Select Interfaces**. By default, the interfaces that have the same name and subnet for the selected target hosts are displayed. However, you can also choose to view all the interfaces for the selected target hosts. You can either select one of the existing interfaces or specify a completely new one if the interface you want to use does not exist.

- b. In the Network Interface Configuration section, review the details of the private and public interfaces.
 - c. Click **Next**.
5. On the Credentials/Schedule page, do the following:
- a. In the Reference Host Credentials section, retain the default selection, that is, **Use Preferred Credentials**.

Note: You can optionally override these preferred credentials. The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Different for each Oracle Home** if you want to use different operating system credentials for each Oracle home, or **Same for all Oracle Homes** if you want to use the same set of credentials for all Oracle homes. Depending on the selection you make, specify the credentials. Ensure that the users belong to the same group (*dba/oinstall*).

- b. In the Target Host(s) Credentials section, provide the credentials as described in Step 6 (a).

Note: If you are using vendor clusterware, then ensure that `root` and the operating system users, such as `oracle` and `crsuser`, owning the clusterware and various Oracle homes are a part of the operating system groups required by the vendor clusterware.

For example, if your system uses High Availability Cluster Multiprocessing (HACMP) clusterware, then create or check for the existence of the group `hagsuser`. Ensure that the relevant operating system users and root user are members of this group.

For more information, refer to the *Oracle Clusterware and Oracle Real Application Clusters Installation and Configuration Guide*.

- c. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
 - d. Click **Next**.
6. On the Configure Cluster page, do the following:
- a. In the Cluster Name and Location section, review the default name and location details provided for Oracle Clusterware and Oracle RAC Database. While Oracle recommends you to retain the default values, you can always edit them to provide custom values.

For security purposes, the clusterware configuration sets the ownership of Oracle Clusterware home and all its parent directories to be owned by `root`. Hence, Oracle recommends you to install Oracle Clusterware outside the Oracle base of the Oracle RAC home.

The default cluster name you see here is based on the host cluster name you provided in the Agent Deploy application in Cloud Control, while deploying Management Agents on a cluster. The scratch location you see here is a temporary location on the target host where temporary files are placed before provisioning and configuring Oracle RAC.

For **Additional Parameters**, specify any additional parameters you want to run while installing Oracle Clusterware. For example, `-debug`.

You can specify any Oracle Universal Installer (OUI) parameter that can be used in this provisioning operation. Using these parameters, you can even change the installation type of the database. For example, `INSTALL_TYPE=SE`. Ensure that the parameters are separated by white space.

Note:

- If you do not see a default cluster name in the **Cluster Name** field, then you might have selected nodes that are not master nodes of the cluster. In this case, manually specify a cluster name, but ensure that the name you specify is the same host cluster name you provided in the Agent Deploy application in Cloud Control, while deploying Management Agents on that cluster.
-
-

- b. In the Database Details section, retain the default selection for creating a starter database.

Note: If the database creation steps are disabled in the Deployment Procedure, then you will not see this section.

If you want to create a general-purpose database, then leave all the fields in this section blank. Otherwise, provide the required details as described in this step.

If you have a custom response file that already has the options enabled, then select **Use response file to create database**, and specify the full path to a location where the file is available. The file may be available on the target host, in a shared location accessible from the target host, in the Software Library, or in a location where an existing database is running.

Note: From the Software Library or from the location where an existing database is running, only a .dbt template file can be used. However, from the target host or a shared location, any template file can be used.

If you do not have a custom response file, then select **Do not use response file**, and provide the global database name, the credentials, and the additional parameters you want to run while creating the starter database.

Note: Ensure that the database name you specify is in the format database_name.database_domain. It must have 1 to 8 alphanumeric characters. For example, orcl.mydomain.com. Also note that the credentials you provide are used for SYS, SYSTEM, SYSMAN, and DBSNMP accounts.

If you want to use the structure of an existing database and have a custom template to structure the new database, then in **Template File for Database**, specify the full path to a location where the template file is available. The file may be available on the target host or on a shared location accessible from the target host.

Note: If you do not store the response files and templates in a central location, you can always customize the Deployment Procedure to add another step that copies the response file or template to the target host before invoking the configuration tools to create the database.

- c. In the Backup and Recovery Details section, retain the default selection, that is, **Do not Enable Automated Backups** if you do not want to have backups taken.

Alternatively, if you want to enable automated backups, select **Enable Automated Backups**, specify the full path to a directory location from where the backed-up files can be recovered, and provide the operating system credentials for running the backup job. Note that recovery location is the same location as the backup location because this where the files are backed up and also recovered from.

- d. In the ASM Instance Details section (appears only if you had selected to deploy ASM), retain the default selection, that is, **Create ASM Instance**, and specify the credentials, additional ASM parameters to be used, and the ASM disk string to be used.

Important: If you are provisioning Oracle Database 10g and Oracle ASM 10g, then ensure that you specify the same password for database as well as ASM.

If you have a custom response file that already has the options enabled, then select **Use response file to create ASM database**, and specify the full path to a location where the file is available. The file may be available on the target host or on a shared location accessible from the target hosts.

If you do not want to use a response file, then select **Do not use response file**.

- e. Click **Next**.
7. On the Storage page, do the following:
 - a. In the Shared Storage Configuration section, provide details about the storage devices and click **Next**. Specify the partition name and the mount location, and select the mount format and a storage device for storing data. While partition name is the path to the location where the device is installed, mount location is the mount point that represents the partition location.

While configuring the storage device, at a minimum, you must have a partition for at least OCR, Voting Disk, and data files. You cannot designate the same storage device to multiple partitions.

Oracle recommends designating the OCR and the OCR Mirror devices to different partitions. Similarly, Oracle recommends designating the Voting Disk, Voting Disk1, and Voting Disk2 to different partitions.

Before clicking **Next**, do the following:

- If you want to clear the data on selected raw devices before creating and configuring the cluster, then select **Clear raw devices**.

- If you have configured only for a few storage devices, then select **Do not provision storage** for others that you do not want to provision.

- Specify the ASM disk string to be used.

- b. In the Options section, select the ASM redundancy mode. The default is None, which requires 7 GB of space. While Normal requires 16 GB of space, High requires 32 GB.

8. (Optional) On the Advanced Configuration page, do the following:

Note: If the configuration steps are disabled in the Deployment Procedure, then you will not see this page.

- a. In the Bonding Interface (Private Interconnect) section, select **Configure Bonding Interface** if you want to configure the bonding interface. To bind the interfaces, specify details as described in [Table 9-2](#).
- b. In the Sysctl File Configuration section, select **Configure Sysctl** file if you want to configure the sysctl.conf file. Specify the mode of editing the system

configuration file and the location of the reference system configuration file used for modifying the kernel parameters.

The default mode is *append*. You can however select *edit* to modify, and *replace* to replace the current `sysctl.conf` file.

Ensure that the reference file you specify is available in a shared location accessible by the Oracle Management Service.

9. On the Review page, review the details you have provided for provisioning Oracle RAC, and click **Submit**. If the details you provided seem to be missing on this page, then see the workaround described in [Appendix E, "Troubleshooting Issues"](#).
10. After the Deployment Procedure ends successfully, instrument the database to collect configuration information.

9.4 Provisioning Oracle Real Application Clusters Using Gold Image

This section describes how you can provision a gold image of Oracle RAC.

Note: Ensure that you use a gold image that was created using the Oracle home directory of a RAC database. You cannot use a gold image that was created using the Oracle home directory of a standalone database.

This section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

9.4.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites.

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Ensure that you create gold images of existing Oracle RAC Database and Oracle Grid Infrastructure.

To understand how you can create a gold image, see [Section 4.3, "Setting Up Database Provisioning"](#).

- Ensure that the target hosts have the necessary hardware and software required for Oracle RAC. The hardware requirements include setting up of the following:
 - Private Network: The network interface cards must be installed on each node and connected to each other.
 - Shared Storage Between Nodes: The shared storage is required for OCR, Voting disks and the data files.
- Ensure that the Virtual IPs are set up in the DNS. If you choose to set up the Virtual IPs locally, then the IP addresses can be specified using the Deployment Procedure, and the procedure will set them up for you.

- If you want to use a custom template to create a structure for the database, then create a template (a `.dbt` file), and store it in a location accessible from the target hosts. The file may be on the target host or on a shared location.

To understand how a template can be created and used for creating databases, see [Section 4.3.7, "Creating Database Templates"](#).

- Ensure that operating system users such as *oracle* and *crsuser* are available on all nodes of the cluster. These users must be a part of the relevant operating system groups such as *dba* and *oinstall*.

For more information, see Oracle Clusterware Installation Guide available at:

<http://www.oracle.com/pls/db111/homepage>

- Ensure that the User IDs for operating system users and the Group IDs for operating system groups are identical on all nodes of the cluster.

Prerequisites for Operators

- Ensure that you do NOT use an NIS-based operating system user.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure and its commands on the target hosts. If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges. For information about customization, see [Chapter 33](#).
- While selecting the source, remember to remove `sqlnet.ora` from the list of files mentioned in **Files to Exclude**.
- Ensure that the `umask` value on the target host is `022`.

9.4.2 Provisioning Procedure

To provision a gold image of an Oracle RAC installation, follow these steps:

1. From the Enterprise menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Provisioning page, select one of the following, and click **Launch**.
 - a. To run the Deployment Procedure on UNIX platforms, Select **Provision Oracle Clusterware / RAC for UNIX and RDBMS versions 10g/11g**.
 - b. To run the Deployment Procedure on Microsoft Windows platforms, select **Provision Oracle Clusterware / RAC for Windows and RDBMS versions 10g/11g**.

Cloud Control displays the Select Source page of the Deployment Procedure.

3. On the Select Source page, do the following:
 - a. In the Select Source section, select **Select from Software Library**.
 - b. In the Source for Clusterware section, click the torch icon and select the generic component that has the gold image of Oracle Clusterware. Ensure that you select only components that are in "Ready" status. Once you select the component name, the application automatically displays the component location.

Note: If you do not see the required component in the Software Library, then follow the workaround described in [Appendix E](#).

- c. In the Source for RAC section, click the torch icon and select the generic component that has the gold image of Oracle Database. Ensure that you select only components that are in "Ready" status. Once you select the component name, the application automatically displays the component location.

Note: If you do not see the required component in the Software Library, then follow the workaround described in [Appendix E](#).

- d. (Optional) In the Source for ASM section, do one of the following:
If you do not want to deploy ASM, then retain the default selection, that is, **Do not Provision ASM**.

If you want to deploy ASM in the same Oracle home as the Oracle RAC, then select **Use the same source as the RAC home**. Alternatively, if you can select **Choose a component** and upload an ASM component from the Software Library.

- e. Click **Next**.

4. On the Select Hosts page, do the following:

- a. In the Hosts to Include in Cluster section, click **Add** and select the target hosts that should form the cluster. To see more details about the selected hosts, click **Show Options**.

Note: When you click **Add**, the Select Target pop-up window appears. On this page, by default, the **Show Suitable Hosts** option is selected and the table lists only those hosts that are best suited for provisioning. If you do not find the host you want to add, then select **Show All Hosts** to view a complete list of hosts.

By default, Private Host Name and Virtual Host Name are automatically prefilled with values. Edit them and specify values that match with your environment. Optionally, you can also specify their IP addresses.

Note: If the prefilled, default values of Private Host Name and Virtual Host Name are incorrect, then see the workaround described in [Appendix E](#).

If you already have these details stored in cluster configuration file, then click **Import From File** to select that cluster configuration file. This file typically contains information about the new hosts to be added. To understand how a cluster configuration file looks, see the sample file shown in [Section 9.5.2.1](#).

To configure the private and public network interfaces, click **Select Interfaces**. By default, the interfaces that have the same name and subnet for the selected target hosts are displayed. However, you can also choose to view all the interfaces for the selected target hosts. You can either select one of the existing

interfaces or specify a completely new one if the interface you want to use does not exist.

- b. In the Network Interface Configuration section, review the details of the private and public interfaces.
 - c. Click **Next**.
5. On the Credentials/Schedule page, do the following:
- a. In the Target Host(s) Credentials section, retain the default selection, that is, **Use Preferred Credentials**.

Note: You can optionally override these preferred credentials. The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Different for each Oracle Home** if you want to use different operating system credentials for each Oracle home, or **Same for all Oracle Homes** if you want to use the same set of credentials for all Oracle homes. Depending on the selection you make, specify the credentials. Ensure that the users belong to the same group (*dba/oinstall*).

Note: If you are using vendor clusterware, then ensure that `root` and the operating system users, such as `oracle` and `crsuser`, owning the clusterware and various Oracle homes are a part of the operating system groups required by the vendor clusterware.

For example, if your system uses High Availability Cluster Multiprocessing (HACMP) clusterware, then create or check for the existence of the group `hagsuser`. Ensure that the relevant operating system users and root user are members of this group.

For more information, refer to the *Oracle Clusterware and Oracle Real Application Clusters Installation and Configuration Guide*.

- b. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
 - c. Click **Next**.
6. On the Configure Cluster page, do the following:
- a. In the Cluster Name and Location section, review the default name and location details provided for Oracle Clusterware and Oracle RAC Database. While Oracle recommends you to retain the default values, you can always edit them to provide custom values.

For security purposes, the clusterware configuration sets the ownership of Oracle Clusterware home and all its parent directories to be owned by *root*. Hence, Oracle recommends you to install Oracle Clusterware outside the Oracle base of the Oracle RAC home.

The default cluster name you see here is based on the host cluster name you provided in the Agent Deploy application in Cloud Control, while deploying Management Agents on a cluster. The scratch location you see here is a temporary location on the target host where temporary files are placed before provisioning and configuring Oracle RAC.

For **Additional Parameters**, specify any additional parameters you want to run while installing Oracle Clusterware. For example, `-debug`.

You can specify any Oracle Universal Installer (OUI) parameter that can be used in this provisioning operation. Using these parameters, you can even change the installation type of the database. For example, `INSTALL_TYPE=SE`. Ensure that the parameters are separated by white space.

- b. In the Database Details section, retain the default selection for creating a starter database.

Note: If the database creation steps are disabled in the Deployment Procedure, then you will not see this section.

If you want to create a general-purpose database, then leave all the fields in this section blank. Otherwise, provide the required details as described in this step.

If you have a custom response file that already has the options enabled, then select **Use response file to create database**, and specify the full path to a location where the file is available. The file may be available on the target host, in a shared location accessible from the target host, in the Software Library, or in a location where an existing database is running.

Note: From the Software Library or from the location where an existing database is running, only a `.dbt` template file can be used. However, from the target host or a shared location, any template file can be used.

If you do not have a custom response file, then select **Do not use response file**, and provide the global database name, the credentials, and the additional parameters you want to run while creating the starter database.

Note: Ensure that the database name you specify is in the format `database_name.database_domain`. It must have 1 to 8 alphanumeric characters. For example, `orcl.mydomain.com`. Also note that the credentials you provide are used for `SYS`, `SYSTEM`, `SYSMAN`, and `DBSNMP` accounts.

If you want to use the structure of an existing database and have a custom template to structure the new database, then in **Template File for Database**, specify the full path to a location where the template file is available. The file

may be available on the target host or on a shared location accessible from the target host.

Note: If you do not store the response files and templates in a central location, you can always customize the Deployment Procedure to add another step that copies the response file or template to the target host before invoking the configuration tools to create the database.

- c. In the Backup and Recovery Details section, retain the default selection, that is, **Do not Enable Automated Backups** if you do not want to have backups taken.

Alternatively, if you want to enable automated backups, select **Enable Automated Backups**, specify the full path to a directory location from where the backed-up files can be recovered, and provide the operating system credentials for running the backup job. Note that recovery location is the same location as the backup location because this where the files are backed up and also recovered from.

- d. In the ASM Instance Details section (appears only if you had selected to deploy ASM), retain the default selection, that is, **Create ASM Instance**, and specify the credentials, additional ASM parameters to be used, and the ASM disk string to be used.

Important: If you are provisioning Oracle Database 10g and Oracle ASM 10g, then ensure that you specify the same password for database as well as ASM.

If you have a custom response file that already has the options enabled, then select **Use response file to create ASM database**, and specify the full path to a location where the file is available. The file may be available on the target host or on a shared location accessible from the target hosts.

If you do not want to use a response file, then select **Do not use response file**.

- e. Click **Next**.
7. On the Storage page, do the following:
- a. In the Shared Storage Configuration section, provide details about the storage devices and click **Next**. Specify the partition name and the mount location, and select the mount format and a storage device for storing data. While partition name is the path to the location where the device is installed, mount location is the mount point that represents the partition location.

While configuring the storage device, at a minimum, you must have a partition for at least OCR, Voting Disk, and data files. You cannot designate the same storage device to multiple partitions.

Oracle recommends designating the OCR and the OCR Mirror devices to different partitions. Similarly, Oracle recommends designating the Voting Disk, Voting Disk1, and Voting Disk2 to different partitions.

Before clicking **Next**, do the following:

- If you want to clear the data on selected raw devices before creating and configuring the cluster, then select **Clear raw devices**.

- If you have configured only for a few storage devices, then select **Do not provision storage** for others that you do not want to provision.
 - Specify the ASM disk string to be used.
 - b. In the Options section, select the ASM redundancy mode. The default is None, which requires 7 GB of space. While Normal requires 16 GB of space, High requires 32 GB.
8. (Optional) On the Configuration page, do the following:

Note: If the configuration steps are disabled in the Deployment Procedure, then you will not see this page.

- a. In the Bonding Interface (Private Interconnect) section, select **Configure Bonding Interface** if you want to configure the bonding interface. To bind the interfaces, specify details as described in [Table 9–2](#).
 - b. In the Sysctl File Configuration section, select **Configure Sysctl** file if you want to configure the sysctl.conf file. Specify the mode of editing the system configuration file and the location of the reference system configuration file used for modifying the kernel parameters.

The default mode is *append*. You can however select *edit* to modify, and *replace* to replace the current sysctl.conf file.

Ensure that the reference file you specify is available in a shared location accessible by the Oracle Management Service.
9. On the Review page, review the details you have provided for provisioning Oracle RAC, and click **Submit**. If the details you provided seem to be missing on this page, then see the workaround described in [Appendix E](#).
10. After the Deployment Procedure ends successfully, instrument the database to collect configuration information.

9.5 Provisioning Oracle Real Application Clusters Using Archived Software Binaries

This section describes how you can provision Oracle RAC that is identical to the one available on the installation medium.

This section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

9.5.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites.

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 9](#).
- Ensure that you upload the software binaries of Oracle RAC Database and Oracle Grid Infrastructure to the Software Library.

- Ensure that the target hosts have the necessary hardware and software required for Oracle RAC. The hardware requirements include setting up of the following:
 - Private Network: The network interface cards must be installed on each node and connected to each other.
 - Shared Storage Between Nodes: The shared storage is required for OCR, Voting disks and the data files.
- Ensure that the Virtual IPs are set up in the DNS. If you choose to set up the Virtual IPs locally, then the IP addresses can be specified using the Deployment Procedure, and the procedure will set them up for you.
- If you want to use a custom template to create a structure for the database, then create a template (a `.dbt` file), and store it in a location accessible from the target hosts. The file may be on the target host or on a shared location.

To understand how a template can be created and used for creating databases, see [Section 4.3.7](#).

- Ensure that operating system users such as *oracle* and *crsuser* are available on all nodes of the cluster. These users must be a part of the relevant operating system groups such as *dba* and *oinstall*.

For more information, see Oracle Clusterware Installation Guide available at:

<http://www.oracle.com/pls/db111/homepage>

- Ensure that the User IDs for operating system users and the Group IDs for operating system groups are identical on all nodes of the cluster.

Prerequisites for Operators

- Ensure that you do NOT use an NIS-based operating system user.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure and its commands on the target hosts. If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges. For information about customization, see [Chapter 33](#).
- Ensure that the `umask` value on the target host is `022`.

9.5.2 Provisioning Procedure

To provision a fresh Oracle RAC installation, follow these steps:

1. From the Enterprise menu, select **Provisioning and Patching** and then select **Database Provisioning**.
2. In the Database Provisioning page, select one of the following, and click **Launch**.
 - a. To run the Deployment Procedure on UNIX platforms, Select **Provision Oracle Clusterware / RAC for UNIX and RDBMS versions 10g/11g**.
 - b. To run the Deployment Procedure on Microsoft Windows platforms, select **Provision Oracle Clusterware / RAC for Windows and RDBMS versions 10g/11g**.

Cloud Control displays the Select Source page of the Deployment Procedure.

3. On the Select Source page, do the following:
 - a. In the Select Source section, select **Select from Software Library**.

- b. In the Source for Clusterware section, click the torch icon and select the generic component that has the software binaries of Oracle Clusterware. Ensure that you select only components that are in "Ready" status. Once you select the component name, the application automatically displays the component location.

Note: If you do not see the required component in the Software Library, then follow the workaround described in [Appendix E](#).

- c. In the Source for RAC section, click the torch icon and select the generic component that has the software binaries of Oracle Database. Ensure that you select only components that are in "Ready" status. Once you select the component name, the application automatically displays the component location.

Note: If you do not see the required component in the Software Library, then follow the workaround described in [Appendix E](#).

- d. (Optional) In the Source for ASM section, do one of the following:

If you do not want to deploy ASM, then retain the default selection, that is, **Do not Provision ASM**.

If you want to deploy ASM in the same Oracle home as the Oracle RAC, then select **Use the same source as the RAC home**. Alternatively, if you can select **Choose a component** and upload an ASM component from the Software Library.

- e. Click **Next**.

4. On the Select Hosts page, do the following:

- a. In the Hosts to Include in Cluster section, click **Add** and select the target hosts that should form the cluster. To see more details about the selected hosts, click **Show Options**.

Note: When you click **Add**, the Select Target pop-up window appears. On this page, by default, the **Show Suitable Hosts** option is selected and the table lists only those hosts that are best suited for provisioning. If you do not find the host you want to add, then select **Show All Hosts** to view a complete list of hosts.

By default, Private Host Name and Virtual Host Name are automatically prefilled with values. Edit them and specify values that match with your environment. Optionally, you can also specify their IP addresses.

Note: If the prefilled, default values of Private Host Name and Virtual Host Name are incorrect, then see the workaround described in [Appendix E](#).

If you already have these details stored in a cluster configuration file, then click **Import From File** to select that cluster configuration file. This file typically contains information about the new hosts to be added. To

understand how a cluster configuration file looks, see the sample file shown in [Section 9.5.2.1](#).

To configure the private and public network interfaces, click **Select Interfaces**. By default, the interfaces that have the same name and subnet for the selected target hosts are displayed. However, you can also choose to view all the interfaces for the selected target hosts. You can either select one of the existing interfaces or specify a completely new one if the interface you want to use does not exist.

- b. In the Network Interface Configuration section, review the details of the private and public interfaces.
 - c. Click **Next**.
5. On the Credentials/Schedule page, do the following:
 - a. In the Target Host(s) Credentials section, retain the default selection, that is, **Use Preferred Credentials**.

Note: You can optionally override these preferred credentials. The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Different for each Oracle Home** if you want to use different operating system credentials for each Oracle home, or **Same for all Oracle Homes** if you want to use the same set of credentials for all Oracle homes. Depending on the selection you make, specify the credentials. Ensure that the users belong to the same group (*dba/oinstall*).

Note: If you are using vendor clusterware, then ensure that `root` and the operating system users, such as `oracle` and `crsuser`, owning the clusterware and various Oracle homes are a part of the operating system groups required by the vendor clusterware.

For example, if your system uses High Availability Cluster Multiprocessing (HACMP) clusterware, then create or check for the existence of the group `hagsuser`. Ensure that the relevant operating system users and root user are members of this group.

For more information, refer to the *Oracle Clusterware and Oracle Real Application Clusters Installation and Configuration Guide*.

- b. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
 - c. Click **Next**.
6. On the Configure Cluster page, do the following:

- a. In the Cluster Name and Location section, review the default name and location details provided for Oracle Clusterware and Oracle RAC Database. While Oracle recommends you to retain the default values, you can always edit them to provide custom values.

For security purposes, the clusterware configuration sets the ownership of Oracle Clusterware home and all its parent directories to be owned by *root*. Hence, Oracle recommends you to install Oracle Clusterware outside the Oracle base of the Oracle RAC home.

The default cluster name you see here is based on the host cluster name you provided in the Agent Deploy application in Cloud Control, while deploying Management Agents on a cluster. The scratch location you see here is a temporary location on the target host where temporary files are placed before provisioning and configuring Oracle RAC.

For **Additional Parameters**, specify any additional parameters you want to run while installing Oracle Clusterware. For example, `-debug`.

You can specify any Oracle Universal Installer (OUI) parameter that can be used in this provisioning operation. Using these parameters, you can even change the installation type of the database. For example, `INSTALL_TYPE=SE`. Ensure that the parameters are separated by white space.

- b. In the Database Details section, retain the default selection for creating a starter database.

Note: If the database creation steps are disabled in the Deployment Procedure, then you will not see this section.

If you want to create a general-purpose database, then leave all the fields in this section blank. Otherwise, provide the required details as described in this step.

If you have a custom response file that already has the options enabled, then select **Use response file to create database**, and specify the full path to a location where the file is available. The file may be available on the target host, in a shared location accessible from the target host, in the Software Library, or in a location where an existing database is running.

Note: From the Software Library or from the location where an existing database is running, only a `.dbt` template file can be used. However, from the target host or a shared location, any template file can be used.

If you do not have a custom response file, then select **Do not use response file**, and provide the global database name, the credentials, and the additional parameters you want to run while creating the starter database.

Note: Ensure that the database name you specify is in the format `database_name.database_domain`. It must have 1 to 8 alphanumeric characters. For example, `orcl.mydomain.com`. Also note that the credentials you provide are used for `SYS`, `SYSTEM`, `SYSMAN`, and `DBSNMP` accounts.

If you want to use the structure of an existing database and have a custom template to structure the new database, then in **Template File for Database**, specify the full path to a location where the template file is available. The file may be available on the target host or on a shared location accessible from the target host.

Note: If you do not store the response files and templates in a central location, you can always customize the Deployment Procedure to add another step that copies the response file or template to the target host before invoking the configuration tools to create the database.

- c. In the Backup and Recovery Details section, retain the default selection, that is, **Do not Enable Automated Backups** if you do not want to have backups taken.

Alternatively, if you want to enable automated backups, select **Enable Automated Backups**, specify the full path to a directory location from where the backed-up files can be recovered, and provide the operating system credentials for running the backup job. Note that recovery location is the same location as the backup location because this where the files are backed up and also recovered from.

- d. In the ASM Instance Details section (appears only if you had selected to deploy ASM), retain the default selection, that is, **Create ASM Instance**, and specify the credentials, additional ASM parameters to be used, and the ASM disk string to be used.

Important: If you are provisioning Oracle Database 10g and Oracle ASM 10g, then ensure that you specify the same password for database as well as ASM.

If you have a custom response file that already has the options enabled, then select **Use response file to create ASM database**, and specify the full path to a location where the file is available. The file may be available on the target host or on a shared location accessible from the target hosts.

If you do not want to use a response file, then select **Do not use response file**.

- e. Click **Next**.
7. On the Storage page, do the following:
- a. In the Shared Storage Configuration section, provide details about the storage devices and click **Next**. Specify the partition name and the mount location, and select the mount format and a storage device for storing data. While partition name is the path to the location where the device is installed, mount location is the mount point that represents the partition location.

While configuring the storage device, at a minimum, you must have a partition for at least OCR, Voting Disk, and data files. You cannot designate the same storage device to multiple partitions.

Oracle recommends designating the OCR and the OCR Mirror devices to different partitions. Similarly, Oracle recommends designating the Voting Disk, Voting Disk1, and Voting Disk2 to different partitions.

Before clicking **Next**, do the following:

- If you want to clear the data on selected raw devices before creating and configuring the cluster, then select **Clear raw devices**.
 - If you have configured only for a few storage devices, then select **Do not provision storage** for others that you do not want to provision.
 - Specify the ASM disk string to be used.
- b. In the Options section, select the ASM redundancy mode. The default is None, which requires 7 GB of space. While Normal requires 16 GB of space, High requires 32 GB.
8. (Optional) On the Configuration page, do the following:

Note: If the configuration steps are disabled in the Deployment Procedure, then you will not see this page.

- a. In the Bonding Interface (Private Interconnect) section, select **Configure Bonding Interface** if you want to configure the bonding interface. To bind the interfaces, specify details as described in [Table 9–2](#).
 - b. In the Sysctl File Configuration section, select **Configure Sysctl** file if you want to configure the sysctl.conf file. Specify the mode of editing the system configuration file and the location of the reference system configuration file used for modifying the kernel parameters.

The default mode is *append*. You can however select *edit* to modify, and *replace* to replace the current sysctl.conf file.

Ensure that the reference file you specify is available in a shared location accessible by the Oracle Management Service.
9. On the Review page, review the details you have provided for provisioning Oracle RAC, and click **Submit**. If the details you provided seem to be missing on this page, then see the workaround described in [Appendix E, "Troubleshooting Issues"](#).
 10. After the Deployment Procedure ends successfully, instrument the database to collect configuration information.

Table 9–2 Configuration Page - Element Description

Element	Description
Bonding Device Name	Specify the name of the bond to be created. For example, bond0
Subnet Mask	Specify the subnet mask for the IP address. For example, 255.255.255.0
Default Gateway	Specify the default gateway for the bonding device. For example, 10.1.2.3
DNS Servers	Specify the Domain Name Server (DNS) list for the bonding device. For multiple DNS servers, the values should be comma-separated. Default values are picked up from the /etc/resolv.conf file. Entries provided here will be appended.
Slave Devices List	Specify the list of slave devices for the bonding device. For multiple slave devices, the values should be comma-separated. For example, eth1,eth2,eth3.

Table 9–2 (Cont.) Configuration Page - Element Description

Element	Description
Bonding Mode	<p>Specifies one of four policies allowed for the bonding module. Acceptable values for this parameter are:</p> <ul style="list-style-type: none"> ■ 0 (Balance-rr)— Sets a round-robin policy for fault tolerance and load balancing. Transmissions are received and sent out sequentially on each bonded slave interface beginning with the first one available. ■ 1 (Active-backup)— Sets an active-backup policy for fault tolerance. Transmissions are received and sent out through the first available bonded slave interface. Another bonded slave interface is only used if the active bonded slave interface fails. ■ 2 (Balance-xor)— Sets an XOR (exclusive-or) policy for fault tolerance and load balancing. Using this method, the interface matches up the incoming request's MAC address with the MAC address for one of the slave NICs. Once this link is established, transmissions are sent out sequentially beginning with the first available interface. ■ 3 (Broadcast)— Sets a round-robin policy for fault tolerance and load balancing. Transmissions are sent out sequentially on each bonded slave interface beginning with the first one available.
Domain Name	Specify the domain name for the assigned host name. For example, foo.com
Primary Slave Device	Specify the interface name, such as eth0, of the primary device. The primary device is the first of the bonding interfaces to be used and is not abandoned unless it fails. This setting is particularly useful when one NIC in the bonding interface is faster and, therefore, able to handle a bigger load. This setting is only valid when the bonding interface is in active-backup mode.
ARP Interval	Specify (in milliseconds) how often ARP monitoring occurs. If using this setting while in mode 0 or 2 (the two load-balancing modes) the network switch must be configured to distribute packets evenly across the NICs. The value is set to 0 by default, which disables it.
MII Interval	Specify (in milliseconds) how often MII link monitoring occurs. This is useful if high availability is required because MII is used to verify that the NIC is active to verify that the driver for a particular NIC supports the MII tool. If using a bonded interface for high availability, the module for each NIC must support MII. Setting the value to 0 (the default), turns this feature off. When configuring this setting, a good starting point for this parameter is 100.
MII Interval Down Delay	Specify (in milliseconds) how long to wait after link failure before disabling the link. The value must be a multiple of the value specified in the miimon parameter. The value is set to 0 by default, which disables it.
MII Interval Up Delay	Specify (in milliseconds) how long to wait before enabling a link. The value must be a multiple of the value specified in the miimon parameter. The value is set to 0 by default, which disables it.
NTP Server	Specify the NTP server for the assigned host name. For example, 1.2.3.4.

9.5.2.1 Sample Cluster Configuration File

The following shows the contents of a typical cluster configuration file:

```
# Cluster Configuration file
```

```
# Node information
```

# Public Node Name	Private Node Name	Private IP (Optional)	Virtual Host Name	Virtual IP (Optional)
node1.domain.com	node1-priv.domain.com	-	node1-vip.domain.com	-
node2.domain.com	node2-priv.domain.com	10.2.109.103	node2-vip.domain.com	134.2.109.103

Extending Oracle Real Application Clusters

This chapter explains how you can extend and scale up an existing Oracle RAC stack (Oracle Clusterware, Oracle ASM, Oracle RAC database), in a single click using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Getting Started](#)
- [Extending Oracle Real Application Clusters](#)

10.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in extending an existing Oracle RAC stack. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully extend an existing Oracle RAC. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 10–1 *Getting Started with Extending Oracle RAC*

Step	Description	Reference Links
Step 1	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	To learn about the prerequisites for extending Oracle RAC, see Section 10.2.1 .
Step 2	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully extend an existing Oracle RAC.</p>	To extend Oracle RAC, follow the steps explained in Section 10.2.2 .

10.2 Extending Oracle Real Application Clusters

This section describes how you can extend an existing Oracle RAC to include as many additional nodes as you need, in just one click.

This section covers the following:

- [Prerequisites](#)
- [Procedure](#)

10.2.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Ensure that *oinstall* and *dba* groups are available.
- Ensure that operating system users such as *oracle* and *crsuser* are available on all nodes of the cluster. These users must be a part of the relevant operating system groups such as *dba* and *oinstall*.
- Ensure that the credentials being used to run this operation along with the group ID are the same on all nodes of the selected cluster.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as *mkdir*, *ls*, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

- Ensure that the shared storage used for existing cluster nodes are accessible to the nodes you want to add.
- Ensure that the *umask* value on the target host is 022. To verify this, run the following command:

```
$ umask
```

Depending on the shell you are using, you can also verify this value in */etc/profile*, */etc/bashrc*, or */etc/csh.cshrc*.

10.2.2 Procedure

To extend an existing Oracle RAC, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Provisioning page, select **Extend Oracle Real Application Clusters** and click **Launch**.

Cloud Control displays the Extend Real Application Clusters page.

3. On the Extend Real Application Clusters page, do the following:

- a. In the Select Real Application Clusters (RAC) section, select the Oracle RAC you want to extend. The associated clusterware and Automatic Storage Management (ASM) also get extended if they are not already existing.

You can use the **Search** section to search for a particular Oracle RAC. From the **Search** list, select the target type based on which you want to search, and click **Go**. You can use wildcards such as % and *.

Note: If the cluster database you want to extend does not appear on this page, then:

- Specify the Clusterware home location for the cluster target in Cloud Control. In Cloud Control, click the **Targets** menu, and then click **All Targets**. On the All Targets page, from the Search list, select **Cluster** and click **Go**. From the results table, select the cluster for which you want to specify the clusterware home location. On the Cluster Home page, click **Monitoring Configuration**. On the Configure Target page, specify the clusterware home location and click **Update**.
 - Configure Cloud Control settings to display them. In Cloud Control, click the **Deployments** tab, and on the Deployments page, in the Configuration section, click **Refresh Host Configuration**. On the following page, from the Available Hosts pane, select the hosts and add them to the **Selected Hosts** pane. Then, click **Refresh Hosts** and wait for the job to succeed. Return to this Deployment Procedure page and run the search query again to view the hosts in the search results.
-

- b. In the Reference Host Options section, from the **Reference Host** list, select a host that you want to use as the primary host for performing this operation. Reference Host is the host that is selected for creation of clone archives and then transferred to the new target nodes being added.

For **Working directory**, specify the full path to an existing directory on the selected host that can be used for staging files for cloning. If the directories you specify do not exist on the target hosts, then they will be created by the Deployment Procedure. Ensure that the working directory is NOT shared on the nodes.

For **Files To Exclude**, for each Oracle home, specify the files you want to exclude while performing this operation. Note that any file or folder corresponding to the regular expressions provided here will be excluded.

- c. In the Oracle Home Shared Storage Options section, select the Oracle home locations that are on shared storage.
- d. In the Select New Nodes section, click **Add** to add new nodes that you want to include to the selected Oracle RAC. After adding the node, specify the virtual node name for each new node and verify the values displayed by default.

Note: Ensure that you select nodes that are monitored by Oracle Management Agents 12c Release 1 (12.1.0.1) or higher.

Optionally, you can click **Show Options** to specify Private Node Name, Private IP, Virtual IP, and Working Directory. **Private Node Name** and

Private IP are required only if you want to set up a private network as part of the procedure. **Virtual Node Name** and **Virtual IP** are required only if they are fixed and not DHCP-based. If the node is already part of the Oracle RAC system, it will be ignored. If the node is part of the Oracle Clusterware, the private network and virtual host information will be ignored. For **Working Directory**, ensure that the location you specify is NOT shared on the nodes.

If you already have these details stored in cluster configuration file, then click **Import From File** to select that cluster configuration file. This file typically contains information about the new nodes to be added. It may also include information about the private node name, private IP address, virtual host name, and virtual IP address to which the Oracle RAC should be extended.

- e. In the User Credentials (Override Preferred Credentials) section, retain the default selection, that is, **Use Preferred Credentials**.

Note: You can optionally override these preferred credentials. For example, if you have added two destination hosts where the users are A and B, then you can choose to override the preferred credentials with different credentials for each of the hosts. Similarly, if the destinations hosts have same credentials, which may be different from the preferred credentials, then you can override the preferred credentials with same credentials for all hosts.

The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Different for each Oracle Home** if you want to use different operating system credentials for each Oracle home, or **Same for all Oracle Homes** if you want to use the same set of credentials for all Oracle homes. Depending on the selection you make, specify the credentials. Ensure that the users belong to the same group (*dba/oinstall*).

Note: If you are using vendor clusterware, then ensure that `root` and the operating system users, such as `oracle` and `crsuser`, owning the clusterware and various Oracle homes are a part of the operating system groups required by the vendor clusterware.

For example, if your system uses High Availability Cluster Multiprocessing (HACMP) clusterware, then create or check for the existence of the group `hagsuser`. Ensure that the relevant operating system users and root user are members of this group.

For more information, refer to the *Oracle Clusterware and Oracle Real Application Clusters Installation and Configuration Guide*.

- f. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
 - g. In the Prerequisites (Run Prerequisites and Fix-Ups) section, by default, **Skip prerequisites and fix-ups** is not selected and therefore, the deployment procedure runs the prerequisite checks and fix-ups on the selected nodes.

The prerequisite checks are required to ensure that the nodes meet all the requirements of this operation and are ready to be added to the cluster. The option is not selected assuming that you have not already run the prerequisite checks on the selected nodes beforehand.

If you have already run the prerequisite checks on the selected nodes and want the deployment procedure to skip running them all over again, then select **Skip prerequisites and fix-ups**.

If you have never run prerequisite checks on the selected nodes and if you want the deployment procedure to run them, then deselect **Skip prerequisites and fix-ups**. The deployment procedure runs the prerequisite checks, fixes issues if there are any, and then proceeds with the extend cluster operation.

If you want to check the prerequisites only but not proceed with the operation at this point, then click **Run Prerequisites Only**.
 - h. Click **Review**.
4. On the Review page, review the details you have provided for extending Oracle RAC, and click **Submit**.

Note: if the Deployment Procedure fails, then review log files described in [Section E.8](#).

Note: When you run the Deployment Procedure on Linux Itanium x64, if the *CVU Run to verify shared locations* step fails, then manually fix it before proceeding to the next step. No automated fix-ups are available for this platform.

Deleting or Scaling Down Oracle Real Application Clusters

This chapter describes how you can delete or scale down Oracle RAC. In particular, this chapter covers the following:

- [Getting Started](#)
- [Core Components Deleted](#)
- [Deleting the Entire Oracle RAC](#)
- [Scaling Down Oracle RAC by Deleting Some of Its Nodes](#)

11.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in deleting or scaling down an existing Oracle RAC stack. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully delete or scale down an existing Oracle RAC stack. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 11–1 *Getting Started with Deleting or Scaling Down an Existing Oracle RAC*

Step	Description	Reference Links
Step 1	<p>Selecting the Use Case</p> <p>This chapter covers a few use cases for deleting and scaling down an existing Oracle RAC. Select the use case that best matches your requirement.</p>	<ul style="list-style-type: none"> ▪ To learn about deleting the entire Oracle RAC stack, see Section 11.3, "Deleting the Entire Oracle RAC". ▪ To learn about scaling down an existing Oracle RAC stack by deleting one or more of its own nodes, see Section 11.4, "Scaling Down Oracle RAC by Deleting Some of Its Nodes".
Step 2	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	<ul style="list-style-type: none"> ▪ To learn about the prerequisites for deleting an entire Oracle RAC stack, see Section 11.3.1, "Prerequisites". ▪ To learn about the prerequisites for scaling down an existing Oracle RAC stack by deleting one or more of its own nodes, see Section 11.4.1, "Prerequisites".

Table 11–1 (Cont.) Getting Started with Deleting or Scaling Down an Existing Oracle

Step	Description	Reference Links
Step 3	Running the Deployment Procedure Run the Deployment Procedure to successfully delete or scale down an existing Oracle RAC.	<ul style="list-style-type: none"> ■ To delete an entire Oracle RAC stack, follow the steps explained in Section 11.3.2, "Procedure". ■ To scale down an existing Oracle RAC stack by deleting one or more of its own nodes, follow the steps explained in Section 11.4.2, "Procedure".

11.2 Core Components Deleted

Using the *Delete/Scale down Oracle Real Application Clusters* Deployment Procedure, you can delete either a node of an existing Oracle RAC or the entire Oracle RAC. As a result, the Deployment Procedure deinstalls the Oracle Clusterware, listeners, and Oracle RAC and ASM homes associated with the nodes selected for deletion.

This Deployment Procedure enables you to descale an entire cluster database stack (Oracle Clusterware, Oracle ASM, and Oracle RAC database) or one or more nodes of an Oracle RAC cluster, in a single click. This includes cluster databases of various releases as described in [Section 4.2](#), and across different platforms.

The procedure can descale or delete clusters that have:

- Oracle CRS, Oracle ASM, and Oracle Database homes owned by the same or different users.
- Separate Oracle CRS, Oracle ASM, and Oracle Database homes present on a shared storage, which is shared by all member nodes.
- Partially provisioned or failed installations of Oracle RAC clusters (may include one or more tiers of the stack installed. For example, cleanup after the clusterware installation failed or cleanup when the clusterware was only partially provisioned).
- Nodes that were reimaged or shut down, and the existing configuration has to be resolved to remove all references to this node in Cloud Control.

11.3 Deleting the Entire Oracle RAC

This section describes how you can delete the entire Oracle RAC. In particular, this section covers the following:

- [Prerequisites](#)
- [Procedure](#)

11.3.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Ensure that *oinstall* and *dba* groups are available.

- Ensure that operating system users such as *oracle* and *crsuser* are available on all nodes of the cluster. These users must be a part of the relevant operating system groups such as *dba* and *oinstall*.
- Ensure that the credentials being used to run this operation along with the group ID are the same on all nodes of the selected cluster.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as *mkdir*, *ls*, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

- REMOVE_ANY_TARGET Enterprise Manager privilege

11.3.2 Procedure

To delete the entire Oracle RAC, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Provisioning page, select **Delete/Scale down Oracle Real Application Clusters** and click **Launch**.

Cloud Control displays the Delete/Scale down Oracle Real Application Clusters page.

3. On the Delete/Scale down Oracle Real Application Clusters page, do the following:
 - a. In the Select Cluster section, click the torch icon for **Select Cluster** and select an Oracle Clusterware instance that you want to delete. Along with the selected Oracle Clusterware, the associated Oracle RAC and ASM instances will also be deleted. The table displays details about the member nodes that are part of the selected Oracle Clusterware.

Note:

When you use the torch icon to search for Oracle Clusterware, if you do not find the Oracle Clusterware that you are looking for, then from the tip mentioned below the table, click **here** to manually provide details about that clusterware and search for it.

This is particularly useful when you want to delete partially-provisioned or configured Oracle Clusterware instances because, by default, when you click the torch icon, only the fully-provisioned clusterware instances appear for selection. In this case, to search, select, and delete the partially-provisioned instances, click **here**, and in the Enter Cluster Details window, manually provide details about the cluster node that contains the partially-provisioned instance and click **OK**. You can then select the host that appears in the Select Nodes to Delete section and mark for deletion.

- b.** In the Reference Host Options section, from the **Cluster Node** list, select a node that you want to use as the primary node for all cleanup operations.
For **Working directory**, specify the full path to an existing directory on the selected node that can be used for staging files temporarily.
- c.** In the Select Nodes to Delete section, click **Mark all** to select all the nodes for deletion. On clicking **Mark all**, you should see a cross icon against all the nodes in the **Deletion** column. These cross icons indicate that the nodes have been selected for deletion.
- d.** In the User Credentials (Override Preferred Credentials) section, retain the default selection, that is, **Use Preferred Credentials**.

Note: You can optionally override these preferred credentials. For example, if you have added two destination hosts where the users are A and B, then you can choose to override the preferred credentials with different credentials for each of the hosts. Similarly, if the destinations hosts have same credentials, which may be different from the preferred credentials, then you can override the preferred credentials with same credentials for all hosts.

For example, if you have added two destination hosts where the users are A and B, then you can choose to override the preferred credentials with different credentials for each of the hosts. Similarly, if the destinations hosts have same credentials, which may be different from the preferred credentials, then you can override the preferred credentials with same credentials for all hosts.

The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Different for each Oracle Home** if you want to use different operating system credentials for each Oracle home, or **Same for all Oracle Homes** if you want to use the same set of credentials for all Oracle homes. Depending on the selection you make, specify the credentials. Ensure that the users belong to the same group (*dba/oinstall*).

- e. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
 - f. Click **Review**.
4. On the Review page, review the details you have provided for deleting Oracle RAC, and click **Submit**.

Note: if the Deployment Procedure fails, then review log files described in [Section E.8](#).

11.4 Scaling Down Oracle RAC by Deleting Some of Its Nodes

This section describes how you can scale down Oracle RAC by deleting one or more nodes that are part of it, and also other nodes that are part of it but do not appear as targets in Cloud Control. In particular, this section covers the following:

- [Prerequisites](#)
- [Procedure](#)

11.4.1 Prerequisites

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Ensure that *oinstall* and *dba* groups are available.
- Ensure that operating system users such as *oracle* and *crsuser* are available on all nodes of the cluster. These users must be a part of the relevant operating system groups such as *dba* and *oinstall*.
- Ensure that the credentials being used to run this operation along with the group ID are the same on all nodes of the selected cluster.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as *mkdir*, *ls*, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

11.4.2 Procedure

To scale down Oracle RAC by deleting one or more nodes that are part of it, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Provisioning page, select **Delete/Scale down Oracle Real Application Clusters** and click **Launch**.

Cloud Control displays the Delete/Scale down Oracle Real Application Clusters page.

3. On the Delete/Scale down Oracle Real Application Clusters page, do the following:
 - a. In the Select Cluster section, click the torch icon for **Select Cluster** and select an Oracle Clusterware instance that you want to scale down. Along with the selected Oracle Clusterware, the associated Oracle RAC and ASM instances will also be deleted. The table displays details about the member nodes that are part of the selected Oracle Clusterware.

Note: When you use the torch icon to search for Oracle Clusterware, if you do not find the Oracle Clusterware that you are looking for, then you can manually provide details about that clusterware and search for it. To do so, from the tip mentioned below the table, click [here](#).

- b. In the Reference Host Options section, from the **Cluster Node** list, select a node that you want to use as the primary node for all cleanup operations.
For **Working directory**, specify the full path to an existing directory on the selected node that can be used for staging files.
- c. In the Select Nodes to Delete section, select the nodes you want to delete, and click **Mark for delete**. On clicking **Mark for delete**, you should see a cross icon against the selected nodes in the **Deletion** column. These cross icons indicate that the nodes have been selected for deletion.

If you do not see the nodes that are part of the cluster, then click **Add more nodes** to add those nodes so that nodes that do not appear as targets in Cloud Control also are selected for deletion.

If you want to deselect a node, click **Unmark**. If you want to select all nodes at a time, click **Mark all**, and if you want to deselect all nodes, click **Unmark all**.

- d. In the User Credentials (Override Preferred Credentials) section, retain the default selection, that is, **Use Preferred Credentials**.

Note: You can optionally override these preferred credentials. For example, if you have added two destination hosts where the users are A and B, then you can choose to override the preferred credentials with different credentials for each of the hosts. Similarly, if the destination hosts have same credentials, which may be different from the preferred credentials, then you can override the preferred credentials with same credentials for all hosts.

The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Different for each Oracle Home** if you want to use different operating system credentials for each Oracle home, or **Same for all Oracle Homes** if you want to use the same set of credentials for all Oracle homes. Depending on the selection you make, specify the credentials. Ensure that the users belong to the same group (*dba/oinstall*).

- e. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
 - f. Click **Review**.
4. On the Review page, review the details you have provided for deleting or scaling down Oracle RAC, and click **Submit**.

Note: if the Deployment Procedure fails, then review log files described in [Section E.8](#).

Provisioning Oracle Database Replay Client

This chapter explains how you can provision Oracle Database Replay Client using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Getting Started](#)
- [Cloning a Running Oracle Database Replay Client](#)
- [Provisioning Oracle Database Replay Client Using Gold Image](#)
- [Provisioning Oracle Database Replay Client Using Installation Binaries](#)

12.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in provisioning Oracle Database Replay Client. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision Oracle Database Replay Client. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 12-1 *Getting Started with Provisioning Oracle Database Replay Client*

Step	Description	Reference Links
Step 1	<p>Selecting the Use Case</p> <p>This chapter covers a few use cases for provisioning Oracle Database Replay Client. Select the use case that best matches your requirement.</p>	<ul style="list-style-type: none"> ▪ To learn about cloning an existing Oracle Database Replay Client, see Section 12.2. ▪ To learn about provisioning Oracle Database Replay Client using a gold image, see Section 12.3. ▪ To learn about provisioning a standalone Oracle Database Replay Client, see Section 12.4.
Step 2	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	<ul style="list-style-type: none"> ▪ To learn about the prerequisites for cloning an existing Oracle Database Replay Client, see Section 12.2.1. ▪ To learn about the prerequisites for provisioning Oracle Database Replay Client using a gold image, see Section 12.3.1. ▪ To learn about the prerequisites for provisioning a standalone Oracle Database Replay Client, see Section 12.4.1.

Table 12–1 (Cont.) Getting Started with Provisioning Oracle Database Replay Client

Step	Description	Reference Links
Step 3	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully provision Oracle Database Replay Client.</p>	<ul style="list-style-type: none"> ▪ To clone an existing Oracle Database Replay Client, follow the steps explained in Section 12.2.2. ▪ To provision Oracle Database Replay Client using a gold image, follow the steps explained in Section 12.3.2. ▪ To provision a standalone Oracle Database Replay Client, follow the steps explained in Section 12.4.2.

12.2 Cloning a Running Oracle Database Replay Client

This section describes how you can clone an existing Oracle Database Replay Client that is running on a host monitored by Cloud Control.

This option is best suited when you have a running instance of Oracle Database Replay Client that is stable and has all the latest patches applied, and you want to make identical copies of it on multiple hosts. However, the risk involved in using an existing instance is that the instance may be deleted or deinstalled anytime without prior notice, and as a result, the Deployment Procedure may fail. Therefore, use this option when you know that the running instance is available for cloning.

In particular, this section covers the following:

- [Prerequisites](#)
- [Cloning Procedure](#)

12.2.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Compare the configuration of the source and target hosts and ensure that they have the same configuration. If the configurations are different, then contact your system administrator and fix the inconsistencies before running the Deployment Procedure.

To compare the configuration of the hosts, in Cloud Control, click **Targets** and then **Hosts**. On the Hosts page, click the name of the source host to access its Home page, and then from the Host menu, click **Configuration** and then click **Compare**.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as `mkdir`, `ls`, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment

Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

- Ensure that the `umask` value on the target host is `022`. To verify this, run the following command:

```
$ umask
```

Depending on the shell you are using, you can also verify this value in `/etc/profile`, `/etc/bashrc`, or `/etc/csh.cshrc`.

12.2.2 Cloning Procedure

To clone an existing instance of Oracle Database Replay Client, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the Provision Oracle Database Client Deployment Procedure and click **Launch**. The Oracle Database Client provisioning wizard is launched.
3. On the Select Source and Destination page, do the following:
 - a. In the Select Source section, select **Existing Database Replay Client Installation**. Then click the torch icon for **Source Host** and select the host on which the existing Oracle Database Replay Client is running.

In the Source Host Details section, by default, **Oracle Home**, **Working Directory**, and **Files to exclude** are prefilled. **Oracle Home** shows where the existing instance is installed, but this is a non-editable field. For **Working Directory**, specify the full path to a directory on source host where the files related to cloning can be staged temporarily. For **Files to exclude**, specify file names that must not be cloned to the source host. Use a comma to separate the file name, and use the wildcard (*) to indicate all files with the same extension. For example, `*.trc`. Note that any file or folder corresponding to the regular expressions provided here will be excluded.

In the Source Host Credentials section, select **Use Preferred Credentials** to use the credentials stored in the Management Repository. Select **Override Preferred Credentials** to specify other credentials.

- b. In the Specify Destination Host Settings section, click **Add** and select the target hosts on which you want to clone the existing instance of Oracle Database Replay Client.

Note: On clicking Add, a window appears with a list of suitable host. If you do not see your desired host, then select **Show All Hosts** and click **Go** to view all other hosts.

By default, **Oracle Base**, **Oracle Home**, and **Working Directory** are prefilled with sample values. Edit them and specify values that match with your environment and standards. If the directories you specify do not exist on the target hosts, then they will be created by the Deployment Procedure.

From the **Credentials** list, retain the default selection, that is, **Preferred**, so that the preferred credentials stored in the Management Repository can be used. Credentials here refer to operating system credentials.

Note: You can optionally override these preferred credentials. For example, if you have added two destination hosts where the users are A and B, then you can choose to override the preferred credentials with different credentials for each of the hosts. Similarly, if the destinations hosts have same credentials, which may be different from the preferred credentials, then you can override the preferred credentials with same credentials for all hosts.

The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

If you have selected multiple hosts, then from the **Path** list, select **Same for all hosts** if you want to use the same path across hosts, or select **Different for each host** if you want to use different paths for each host.

Note: If you select **Same for all hosts**, then ensure that the Oracle home and the user are present on all the hosts.

If you want to customize the host settings, then click **Customize Host Settings**. For example, you can specify the Management Agent home credentials, a name for your installation, or an alternate host name instead of the first host name found on the system.

- c. (Optional) In the Advanced Installation Parameters section, specify any additional parameters you want to run while installing the Oracle Database Replay Client. For example, `-force` (to override any warnings), `-debug` (to view more debug information), and `-invPtrLoc <Location>` (for UNIX only). Ensure that the parameters are separated by white space.

While installing software binaries from an existing Oracle Database Replay Client location, if you want to also stage them to a shared location, then select **Stage to Shared Location** and specify a location that is shared across all destination hosts. This staged location can also act as a source for future deployments.

- d. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
 - e. Click **Continue**.
4. On the Review page, review the details you have provided for provisioning an Oracle Database Replay Client, and click **Submit**.

Note: if the Deployment Procedure fails, then review log files described in [Section E.8](#).

12.3 Provisioning Oracle Database Replay Client Using Gold Image

This section describes how you can provision a gold image of Oracle Database Replay Client from the Software Library.

This option is best suited when you have a copy of a stable, well-tested, and patched Oracle Database Replay Client stored in the Software Library. This option scores over a fresh installation because you save time in patching and testing a fresh instance.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

12.3.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Ensure that the gold image is available either in the Software Library or in a shared, staging location.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as *mkdir*, *ls*, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

- Ensure that you use an operating system user that has *write* permission on the staging areas used for placing software binaries of Oracle Database Replay Client.

Deployment Procedures allow you to use staging locations for quick file-transfer of binaries and prevent high traffic over the network. While providing a staging location, ensure that the operating system user you use has *write* permission on those staging locations.

- Ensure that the *umask* value on the target host is 022. To verify this, run the following command:

```
$ umask
```

Depending on the shell you are using, you can also verify this value in `/etc/profile`, `/etc/bashrc`, or `/etc/csh.cshrc`.

12.3.2 Provisioning Procedure

To provision a gold image of Oracle Database Replay Client from the software library, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the Provision Oracle Database Client Deployment Procedure and click **Launch**. The Oracle Database Client provisioning wizard is launched.
3. On the Deployment Procedure Manager page, in the Procedures subtab, from the table, select **Oracle Database Replay Client Provisioning**. Then click **Schedule Deployment**.

Cloud Control displays the Select Source and Destination page of the Deployment Procedure.

4. On the Select Source and Destination page, do the following:
 - a. In the Select Source section, do one of the following:

If the gold image is stored as a component in the Software Library, then select **Software Library**. Then, click the torch icon for **Component** and select the component that has the gold image. Ensure that you select only components that are in "Ready" status.

Note: If you do not see the required component in the Software Library, then follow the workaround described in [Appendix E](#).

If the gold image was stored as an image in a staging location while provisioning a database in the past, then select **External Staging Server** and then **Gold Image**. Click the torch icon for **Select Host** and select the host where the gold image is stored. Then click the torch icon for **Stage Location** and select the location on the host where the gold image is available. For Product version, specify the version of the product you are provisioning.

- b. In the Specify Destination Host Settings section, click **Add** and select the target hosts on which you want to install the gold image of Oracle Database Replay Client.

Note: On clicking Add, a window appears with a list of suitable host. If you do not see your desired host, then select **Show All Hosts** and click **Go** to view all other hosts.

By default, **Oracle Base**, **Oracle Home**, and **Working Directory** are prefilled with sample values. Edit them and specify values that match with your environment and standards. If the directories you specify do not exist on the target hosts, then they will be created by the Deployment Procedure.

From the **Credentials** list, retain the default selection, that is, **Preferred**, so that the preferred credentials stored in the Management Repository can be used. Credentials here refer to operating system credentials.

Note: You can optionally override these preferred credentials. For example, if you have added two destination hosts where the users are A and B, then you can choose to override the preferred credentials with different credentials for each of the hosts. Similarly, if the destinations hosts have same credentials, which may be different from the preferred credentials, then you can override the preferred credentials with same credentials for all hosts.

The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

If you have selected multiple hosts, then from the **Path** list, select **Same for all hosts** if you want to use the same path across hosts, or select **Different for each host** if you want to use different paths for each host.

Note: If you select **Same for all hosts**, then ensure that the Oracle home and the user are present on all the hosts.

If you want to customize the host settings, then click **Customize Host Settings**. For example, you can specify the Management Agent home credentials, a name for your installation, or an alternate host name instead of the first host name found on the system.

- c. (Optional) In the Advanced Installation Parameters section, specify any additional parameters you want to run while installing the Oracle Database Replay Client. For example, `-force` (to override any warnings), `-debug` (to view more debug information), and `-invPtrLoc <Location>` (for UNIX only). Ensure that the parameters are separated by white space.

While installing the Oracle Database Replay Client location, if you want to also stage them to a shared location, then select **Stage to Shared Location** and specify a location that is shared across all destination hosts. This staged location can also act as a source for future deployments.
 - d. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
 - e. Click **Continue**.
5. On the Review page, review the details you have provided for provisioning an Oracle Database Replay Client, and click **Submit**.

Note: if the Deployment Procedure fails, then review log files described in [Section E.8](#).

12.4 Provisioning Oracle Database Replay Client Using Installation Binaries

This section describes how you can provision Oracle Database Replay Client that is identical to the one available on the installation medium.

This option is best suited when you want a completely new installation to be provisioned across multiple hosts. Of course, understandably, this is a fresh installation and you will have to update it with all the latest patches that have been released so far.

Note: The Oracle Database Replay Client version to be used for replaying workload must be the same version as the version of the test database on which the workload has to be replayed. Oracle Database Replay Client is supported in Oracle Database 10g Release 4 (10.2.0.4) and higher. While you can use archived software binaries for installing Oracle Database Client 11g Release 1 (11.1.0.6) and Oracle Database Client 11g Release 2, for test database versions 10.2.0.4, 10.2.0.5, and 11.1.0.7, you must create a gold image of the respective versions of Oracle Database Replay Client homes and use the same.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

12.4.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).

Note: If you want to create a component for the software binaries of Oracle Database Replay Client, then before you access the Software Library, see My Oracle Support note 815567.1. This note explains the different requirements for each OS platform prior to using the media with Cloud Control Deployment Procedure.

Note: If you want to create a component for the software binaries of Oracle Database Replay Client, do not save the shiphome or component to the Components folder in Software Library. Create a new folder in Software Library and then save the component.

- Ensure that the installation binaries are downloaded, and archived and uploaded as a component in the Software Library.
- Compare the configuration of the source and target hosts and ensure that they have the same configuration. If the configurations are different, then contact your system administrator and fix the inconsistencies before running the Deployment Procedure.

To compare the configuration of the hosts, in Cloud Control, click **Targets** and then **Hosts**. On the Hosts page, click the name of the source host to access its Home page, and then from the Host menu, click **Configuration** and then click **Compare**.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as `mkdir`, `ls`, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

- Ensure that the `umask` value on the target host is 022. To verify this, run the following command:

```
$ umask
```

Depending on the shell you are using, you can also verify this value in `/etc/profile`, `/etc/bashrc`, or `/etc/csh.cshrc`.

12.4.2 Provisioning Procedure

To provision a fresh Oracle Database Replay Client, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the Provision Oracle Database Client Deployment Procedure and click **Launch**. The Oracle Database Replay Client provisioning wizard is launched.

Cloud Control displays the Select Source and Destination page of the Deployment Procedure.

3. On the Select Source and Destination page, do the following:

- a. In the Select Source section, do one of the following:

If the software binaries are stored as a component in the Software Library, then select **Software Library**. Then, click the torch icon for **Component** and select the component that has the archived software binaries. Ensure that you select only components that are in "Ready" status. When you select a component from the Software Library, Cloud Control automatically populates the component location.

Note: If you do not see the required component in the Software Library, then follow the workaround described in [Appendix E](#).

If the software binaries are stored as an archived file in a staging location, then select **External Staging Server** and then **Shiphome**. Click the torch icon for **Select Host** and select the host where the archived file is stored. Then click the torch icon for **Stage Location** and select the location on the host where the archived file is available. For Product version, specify the version of the product you are provisioning.

- b. In the Specify Destination Host Settings section, click **Add** and select the target hosts on which you want to install the Oracle Database Replay Client.

Note: On clicking Add, a window appears with a list of suitable host. If you do not see your desired host, then select **Show All Hosts** and click **Go** to view all other hosts.

By default, **Oracle Base**, **Oracle Home**, and **Working Directory** are prefilled with sample values. Edit them and specify values that match with your environment and standards. If the directories you specify do not exist on the target hosts, then they will be created by the Deployment Procedure.

From the **Credentials** list, retain the default selection, that is, **Preferred**, so that the preferred credentials stored in the Management Repository can be used. Credentials here refer to operating system credentials.

Note: You can optionally override these preferred credentials. For example, if you have added two destination hosts where the users are A and B, then you can choose to override the preferred credentials with different credentials for each of the hosts. Similarly, if the destinations hosts have same credentials, which may be different from the preferred credentials, then you can override the preferred credentials with same credentials for all hosts.

The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

If you have selected multiple hosts, then from the **Path** list, select **Same for all hosts** if you want to use the same path across hosts, or select **Different for each host** if you want to use different paths for each host.

Note: If you select **Same for all hosts**, then ensure that the Oracle home and the user are present on all the hosts.

If you want to customize the host settings, then click **Customize Host Settings**. For example, you can specify the Management Agent home

credentials, a name for your installation, or an alternate host name instead of the first host name found on the system.

- c. (Optional) In the Advanced Installation Parameters section, specify any additional parameters you want to run while installing the Oracle Database Replay Client. For example, `-force` (to override any warnings), `-debug` (to view more debug information), and `-invPtrLoc <Location>` (for UNIX only). Ensure that the parameters are separated by white space.

While installing software binaries from the Software Library, if you want to also stage them to a shared location, then select **Stage to Shared Location** and specify a location that is shared across all destination hosts. This staged location can also act as a source for future deployments.

- d. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
 - e. Click **Continue**.
4. On the Review page, review the details you have provided for provisioning an Oracle Database Replay Client, and click **Submit**.

Note: if the Deployment Procedure fails, then review log files described in [Section E.8](#).

Creating Databases

This chapter explains how you can create databases using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Getting Started](#)
- [Creating Oracle Database](#)
- [Creating Oracle Real Application Clusters Database](#)
- [Creating Oracle Real Application Clusters One Node Database](#)

13.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in creating databases. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully create a database using Cloud Control. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 13–1 *Getting Started with Creating Oracle Databases*

Step	Description	Reference Links
Step 1	<p>Selecting the Use Case</p> <p>This chapter covers a few use cases for creating databases. Select the use case that best matches your requirement.</p>	<ul style="list-style-type: none"> ▪ To learn about creating Oracle Single Instance Database, see Section 13.2. ▪ To learn about creating Oracle RAC Database, see Section 13.3. ▪ To learn about creating Oracle RAC One Node Database, see Section 13.4.
Step 2	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	<ul style="list-style-type: none"> ▪ To learn about prerequisites in creating Oracle Database, see Section 13.2.1. ▪ To learn about prerequisites in creating Oracle RAC Database, see Section 13.3.2. ▪ To learn about prerequisites in creating Oracle RAC One Node Database, see Section 13.4.1.
Step 3	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully create the database.</p>	<ul style="list-style-type: none"> ▪ To create Single Instance Database, see Section 13.2.2. ▪ To create Oracle RAC Database, see Section 13.3.2. ▪ To create Oracle RAC One Node Database, see Section 13.4.2.

13.2 Creating Oracle Database

This section provides information about creating Oracle Database (also called single-instance database).

This section covers the following:

- [Prerequisites for Creating Oracle Database](#)
- [Procedure for Creating Oracle Database](#)

13.2.1 Prerequisites for Creating Oracle Database

To create single-instance databases using Cloud Control, ensure that you meet the following prerequisites:

1. Ensure that you meet the infrastructure requirements explained in [Chapter 2](#).
2. Ensure that you have created and stored a database template in the Software Library or Oracle Home. For information about creating database templates, see [Section 4.3.7](#).
3. Oracle Home for the database you want to create must be installed and you need to have credentials of the owner of the Oracle Home. If the Create Database wizard is launched from the Provision Database deployment procedure wizards, the Oracle Home need not be installed earlier. In such cases, the validations for Oracle Home will be skipped during the procedure interview and will be performed during execution of the deployment procedure.
4. Database plug-in that supports the corresponding database version should be deployed on OMS and Agent. For information about deploying plug-ins, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
5. Ensure that you have sufficient space to create the database and write permissions to recovery file location.
6. If you are using a template from the Software Library for database creation, you must have Write permission to the Staging Location.
7. If you are using Automatic Storage Management (ASM) as storage, ASM instances and diskgroups must be configured prior to creating database.
8. The Cloud Control user creating the database template must have CONNECT_ANY_TARGET privilege in Cloud Control.

13.2.2 Procedure for Creating Oracle Database

Follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Provisioning page, select the Create Oracle Database Deployment Procedure and click **Launch**. The Create Oracle Database wizard is launched.
3. In the Database Version and Type page, select the database **Version** and select **Oracle Single Instance Database**.

In the Hosts section, specify hosts and Oracle Home to provision the database. You can also specify Host Credentials and Common Oracle Home across all hosts. The Host Credentials can be Named or Preferred Credentials.

Click the plus (+) icon to add the host. Select the host and specify **Oracle Home**. Select **Host Credentials** or add new. Click the plus icon to add new credentials and specify **User Name**, **Password**, and **Run Privileges** and save the credentials.

Click **Next**.

4. In the Database Template page, choose the database template location. The location can be Software Library or Oracle Home. The template selected must be compatible with the selected Oracle Home version.

If you have selected **Software Library**, click on the search icon and select the template from the Software Library. Specify **Temporary Storage Location on Managed Host(s)**. This location must exist on all hosts where you want to create the database.

Click **Show Template Details** to view details of the selected template. You can view initialization parameters, table spaces, data files, redo log groups, common options, and other details of the template.

If you have selected **Oracle Home**, select the template from the Oracle Home. The default location is `ORACLE_HOME/assistants/dbca/templates`.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

5. In the Identification and Placement page, specify database configuration details. Specify **Global Database Name** and **SID** prefix. Specify the **Database Credentials** for SYS, SYSTEM, and DBSNMP database accounts.

Note:

- SID must be unique for a database on a host. This means, the SID assigned to one database on a host cannot be reused on another database on the same host, but can be reused on another database on a different host. For example, if you have two databases (db1 and db2) on a host (host1), then their SIDs need to be unique. However, if you install the third database on another host (host2), then its SID can be db1 or db2.
 - Global database name must be unique for a database on a host and also unique for databases across different hosts. This means, the global database name assigned to one database on a host can neither be reused on another database on the same host nor on another database on a different host. For example, if you have two databases (db1 and db2) on a host (host1), then their global database names need to be unique. And if you install the third database on another host (host2), the global database name of even this database must be unique and different from all other names registered with Cloud Control.
 - The database credentials you specify here will be used on all the destination hosts. However, after provisioning, if you want to change the password for any database, then you must change it manually.
-
-

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

6. In the Storage Locations page, select the storage type, whether File System or Automatic Storage Management (ASM).

If you want to use a file system, then select **File System** and specify the full path to the location where the data file is present. For example, %ORACLE_BASE%/oradata or /u01/product/db/oradata.

If you want to use ASM, then select **Automatic Storage Management (ASM)**, and click the torch icon to select the disk group name and specify ASMSNMP password. The Disk Group Name List window appears and displays the disk groups that are common on all the destination hosts.

In the Database Files Location section, specify the location where data files, temporary files, redo logs, and control files will be stored.

- Select **Use Database File Locations from Template** to select defaults from the template used.
- Select **Use Common Location for All Database Files** to specify a different location.

If you select **Use Oracle Managed Files (OMF)**, in the Multiplex Redo Logs and Control Files section, you can specify locations to store duplicate copies of redo logs and control files. Multiplexing provides greater fault-tolerance. You can specify up to five locations.

In the Recovery Files Location section, select **Use same storage type as database files location** to use the same storage type for recovery files as database files. Select **Use Flash Recovery Area** and specify the location for recovery-related files and Fast Recovery Area Size.

Select **Enable Archiving** to enable archive logging. Click **Specify Archive Log Locations** and specify up to nine archive log locations. If the log location is not specified, the logs will be saved in the default location.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

7. In the Initialization Parameters page, select the memory management type as **Automatic Memory Management** or **Automatic Shared Memory Management**. Select **Specify Memory Settings as Percentage of Available Memory** to specify memory settings as percentage of available physical memory. For Automatic Shared Memory management, specify **Total SGA** and **Total PGA**. For Automatic Memory Management, specify **Total Memory for Oracle**.

In the Database sizing section, specify the **Block Size** and number of **Processes**. If you have selected a database template with datafiles in the Database Template page, you cannot edit the Block Size.

Specify the Host CPU Count. The maximum CPU count that can be specified is equal to the number of CPUs present on the host.

In the Character Sets section, select the default character set. The default character set is based on the locale and operating system.

Select a national character set. The default is **AL16UTF16**.

In the Database Connection Mode section, select the dedicated server mode. For shared server mode, specify the number of shared servers.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

8. In the Additional Configuration Options, all the available listeners running from the Oracle Home and Grid Infrastructure listeners are listed. You can either select a listener or create a new one. You can select multiple listeners to register with the database. To create a new listener, specify the **Listener Name** and **Port**. Select database schemas and specify custom scripts, if any. Select custom scripts from the host where you are creating the database or from Software Library. If you have selected multiple hosts, you can specify scripts only from Software Library.

If you have selected a Structure Only database template in the Database Template page, you can also view and edit database options.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

9. In the Schedule page, specify a Deployment Instance name and a schedule for the deployment. If you want to run the procedure immediately, then retain the default selection, that is Immediately. If you want to run the procedure later, then select Later and provide time zone, start date, and start time details. Click **Next**.
10. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment. Click **Analyze** to check for prerequisites and to ensure that all the necessary requirements for provisioning are met.
11. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the Status link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

13.3 Creating Oracle Real Application Clusters Database

This section provides information about creating Oracle Real Application Clusters Database.

This section covers the following:

- [Prerequisites for Creating Oracle Real Application Clusters Database](#)
- [Procedure for Creating Oracle Real Application Clusters Database](#)

13.3.1 Prerequisites for Creating Oracle Real Application Clusters Database

To create Oracle RAC databases using Cloud Control, ensure that you meet the following prerequisites:

1. Ensure that you meet the mandatory infrastructure requirements explained in [Chapter 2](#).
2. Ensure that you have created and stored the database template in the Software Library or Oracle Home. For information about creating database templates, see [Section 4.3.7](#).

3. Oracle Home for the database you want to create must be installed and you need to have credentials of the owner of the Oracle Home. If the Create Database wizard is launched from the Provision Database deployment procedure wizards, the Oracle Home need not be installed earlier. In such cases, the validations for Oracle Home will be skipped during the procedure interview and will be performed during execution of the deployment procedure.
4. Database plug-in that supports the corresponding database version should be deployed on OMS and Agent. For information about deploying plug-ins, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
5. Ensure that you have sufficient space to create the database and write permissions to recovery file location.
6. If you are using a template from the Software Library for database creation, you must have Write permission to the Staging Location.
7. If you are creating Oracle Real Application Clusters database, you must have Grid Infrastructure installed and configured. If the Create Database wizard is launched from the Provision Database deployment procedure wizards, Grid Infrastructure need not be installed and configured. In such cases, the validations for Grid Infrastructure will be skipped during the procedure interview and will be performed during execution of the deployment procedure.
8. If you are using Automatic Storage Management (ASM) as storage, ASM instances and diskgroups must be configured prior to creating database.
9. The Cloud Control user creating the database template must have `CONNECT_ANY_TARGET` privilege in Cloud Control.

13.3.2 Procedure for Creating Oracle Real Application Clusters Database

Follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Provisioning page, select the Create Oracle Database Deployment Procedure and click **Launch**. The Create Oracle Database wizard is launched.
3. In the Database Version and Type page, select the database **Version** and select **Oracle Real Application Clusters (Oracle RAC) Database**.

In the Cluster section, select the Cluster and Oracle Home. Select a reference host to perform validations to use as reference to create database on the cluster.

Select **Cluster Credentials** or add new. Click the plus icon to add new credentials and specify **User Name**, **Password**, and **Run Privileges** and save the credentials.

Click **Next**.

4. In the Database Template page, choose the database template location. The location can be Software Library or Oracle Home. The template selected must be compatible with the selected Oracle Home version.

If you have selected **Software Library**, click on the search icon and select the template from the Software Library. Specify **Temporary Storage Location on Managed Host(s)**. This location must be present on the reference node that you selected earlier.

Click **Show Template Details** to view details of the selected template. You can view initialization parameters, table spaces, data files, redo log groups, common options, and other details of the template.

If you have selected **Oracle Home**, select the template from the Oracle Home. The default location is ORACLE_HOME/assistants/dbca/templates.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

5. In the Identification and Placement page, select the type of Oracle RAC database, whether Policy Managed or Admin Managed.

For admin-managed database, select nodes on which you want to create the cluster database. You must specify the node selected as the reference node in the Database Version and Type page.

For policy-managed database, select the server pools to be used for creating the database, from the list of existing server pools, or choose to create a new server pool. Policy-managed databases can be created for database versions 11.2 and higher. For database versions lower than 11.2, you will need to select nodes to create the Oracle RAC database.

Specify **Global Database Name** and **SID** prefix. Specify the **Database Credentials** for SYS, SYSTEM, and DBSNMP.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

6. In the Storage Locations page, select the storage type, whether File System or Automatic Storage Management (ASM).

In the Database Files Location section, specify the location where data files, temporary files, redo logs, and control files will be stored. These locations must be on shared storage such as cluster file system location or ASM diskgroups.

- Select **Use Database File Locations from Template** to select defaults from the template used.
- Select **Use Common Location for All Database Files** to specify a different location.

If you select **Use Oracle Managed Files (OMF)**, in the Multiplex Redo Logs and Control Files section, you can specify locations to store duplicate copies of redo logs and control files. Multiplexing provides greater fault-tolerance. You can specify upto five locations.

In the Recovery Files Location section, select **Use Flash Recovery Area** and specify the location for recovery-related files and Fast Recovery Area Size.

In the Archive Log Settings section, select **Enable Archiving** to enable archive logging. In the Specify Archive Log Locations, you can specify upto nine archive log locations. If the log location is not specified, the logs will be saved in the default location.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

7. In the Initialization Parameters page, select the memory management type as **Automatic Memory Management** or **Automatic Shared Memory Management**. Select **Specify Memory Settings as Percentage of Available Memory** to specify memory settings as percentage of available physical memory. For Automatic

Shared Memory management, specify **Total SGA** and **Total PGA**. For Automatic Memory Management, specify **Total Memory for Oracle**.

In the Database sizing section, specify the **Block Size** and number of **Processes**. If you have selected a database template with datafiles in the Database Template page, you cannot edit the Block Size.

Specify the Host CPU Count. The maximum CPU count that can be specified is equal to the number of CPUs present on the host.

In the Character Sets section, select the default character set. The default character set is based on the locale and operating system.

Select a national character set. The default is **AL16UTF16**.

In the Database Connection Mode section, select the dedicated server mode. For shared server mode, specify the number of shared servers.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

8. In the Additional Configuration Options page, select custom scripts from the Software Library. If you have selected a Structure Only database template in the Database Template page, you can also view and edit database options.

Click on the Lock icon to lock the field. Click **Next**.

9. In the Schedule page, specify a Deployment Instance name and a schedule for the deployment. If you want to run the procedure immediately, then retain the default selection, that is Immediately. If you want to run the procedure later, then select Later and provide time zone, start date, and start time details. Click **Next**.
10. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment. Click **Analyze** to check for prerequisites and to ensure that all the necessary requirements for provisioning are met.
11. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the Status link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

13.4 Creating Oracle Real Application Clusters One Node Database

This section provides information about creating Oracle Real Application Clusters One Node Database (also called as Oracle RAC One Node Database).

This section covers the following:

- [Prerequisites for Creating Oracle RAC One Node Database](#)
- [Procedure for Creating Oracle Real Application Clusters One Node Database](#)

13.4.1 Prerequisites for Creating Oracle RAC One Node Database

To create Oracle RAC One databases using Cloud Control, ensure that you meet the following prerequisites:

1. Ensure that you meet the infrastructure requirements explained in [Chapter 2](#).
2. Ensure that you have created and stored the database template in the Software Library or Oracle Home. For information about creating database templates, see [Section 4.3.7](#).
3. Oracle Home for the database you want to create must be installed and you need to have credentials of the owner of the Oracle Home. If the Create Database wizard is launched from the Provision Database deployment procedure wizards, the Oracle Home need not be installed earlier. In such cases, the validations for Oracle Home will be skipped during the procedure interview and will be performed during execution of the deployment procedure.
4. Database plug-in that supports the corresponding database version should be deployed on OMS and Agent. For information about deploying plug-ins, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.
5. Ensure that you have sufficient space to create the database and write permissions to recovery file location.
6. If you are using a template from the Software Library for database creation, you must have Write permission to the Staging Location.
7. If you are creating Oracle Real Application Clusters database, you must have Grid Infrastructure installed and configured. If the Create Database wizard is launched from the Provision Database deployment procedure wizards, Grid Infrastructure need not be installed and configured. In such cases, the validations for Grid Infrastructure will be skipped during the procedure interview and will be performed during execution of the deployment procedure.
8. If you are using Automatic Storage Management (ASM) as storage, ASM instances and diskgroups must be configured prior to creating database.
9. The Cloud Control user creating the database template must have CONNECT_ANY_TARGET privilege in Cloud Control.

13.4.2 Procedure for Creating Oracle Real Application Clusters One Node Database

Follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Provisioning page, select the Create Oracle Database Deployment Procedure and click **Launch**. The Create Oracle Database wizard is launched.
3. In the Database Version and Type page, select the database **Version** and select **Oracle RAC One Node Database**.

In the Cluster section, select the cluster and Oracle Home. Select a reference host to perform validations to use as reference to create database on the cluster.

Select **Cluster Credentials** or add new. Click the plus icon to add new credentials and specify **User Name**, **Password**, and **Run Privileges** and save the credentials.

Click **Next**.

4. In the Database Template page, choose the database template location. The location can be Software Library or Oracle Home. The template selected must be compatible with the selected Oracle Home version.

If you have selected **Software Library**, click on the search icon and select the template from the Software Library. Specify **Temporary Storage Location on**

Managed Host(s). This location must be present on the reference node that you selected earlier.

Click **Show Template Details** to view details of the selected template. You can view initialization parameters, table spaces, data files, redo log groups, common options, and other details of the template.

If you have selected **Oracle Home**, select the template from the Oracle Home. The default location is ORACLE_HOME/assistants/dbca/templates.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

5. In the Identification and Placement page, select nodes on which you want to create the cluster database. Specify **Global Database Name** and **SID** prefix. Specify the **Database Credentials** for SYS, SYSTEM, and DBSNMP database accounts. Select the type of Oracle RAC database, whether Policy Managed or Admin Managed. Specify the **Service Name**.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

6. In the Storage Locations page, select the storage type, whether File System or Automatic Storage Management (ASM).

In the Database Files Location section, specify the location where data files, temporary files, redo logs, and control files will be stored.

- Select **Use Database File Locations from Template** to select defaults from the template used.
- Select **Use Common Location for All Database Files** to specify a different location.

If you select **Use Oracle Managed Files (OMF)**, in the Multiplex Redo Logs and Control Files section, you can specify locations to store duplicate copies of redo logs and control files. Multiplexing provides greater fault-tolerance. You can specify upto five locations.

In the Recovery Files Location section, select **Use Flash Recovery Area** and specify the location for recovery-related files and Fast Recovery Area Size.

In the Archive Log Settings section, select **Enable Archiving** to enable archive logging. In the Specify Archive Log Locations, you can specify upto nine archive log locations. If the log location is not specified, the logs will be saved in the default location.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

7. In the Initialization Parameters page, select the memory management type as **Automatic Memory Management** or **Automatic Shared Memory Management**. Select **Specify Memory Settings as Percentage of Available Memory** to specify memory settings as percentage of available physical memory. For Automatic Shared Memory management, specify **Total SGA** and **Total PGA**. For Automatic Memory Management, specify **Total Memory for Oracle**.

In the Database sizing section, specify the **Block Size** and number of **Processes**. If you have selected a database template with datafiles in the Database Template page, you cannot edit the Block Size.

Specify the Host CPU Count. The maximum CPU count that can be specified is equal to the number of CPUs present on the host.

In the Character Sets section, select the default character set. The default character set is based on the locale and operating system.

Select a national character set. The default is **AL16UTF16**.

In the Database Connection Mode section, select the dedicated server mode. For shared server mode, specify the number of shared servers.

Click on the Lock icon to lock the fields you have configured. These fields will not be available for editing in the operator role.

Click **Next**.

8. In the Additional Configuration Options page, select custom scripts from the Software Library. If you have selected a Structure Only database template in the Database Template page, you can also view and edit database options. Click on the Lock icon to lock the field. Click **Next**.
9. In the Schedule page, specify a Deployment Instance name and a schedule for the deployment. If you want to run the procedure immediately, then retain the default selection, that is Immediately. If you want to run the procedure later, then select Later and provide time zone, start date, and start time details. Click **Next**.
10. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment. Click **Analyze** to check for prerequisites and to ensure that all the necessary requirements for provisioning are met.
11. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the Status link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

Part IV

Database Upgrade

This part contains the following chapter:

- [Chapter 14, "Upgrading Databases"](#)

Upgrading Databases

This chapter explains how you can upgrade Oracle databases using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Getting Started](#)
- [Deployment Procedure](#)
- [Supported Releases](#)
- [Upgrading Multiple Oracle Database Instances at a Time \(Mass Upgrade\)](#)
- [Upgrading One Oracle Database or One Oracle RAC Database Instance at a Time](#)

14.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in mass upgrade of databases or when you want to install Oracle Home and upgrade database. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully upgrade Oracle database. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 14–1 Getting Started with Upgrading Database

Step	Description	Reference Links
Step 1	<p>Selecting the Usecase</p> <p>Decide whether you want to upgrade single instance database or Oracle RAC database instance, and then select the type of upgrade you want to perform on them.</p> <p>Oracle Database (single-instance database)</p> <p>You can upgrade multiple database instances at a time (mass upgrade). For mass upgrade, you can:</p> <ul style="list-style-type: none"> ▪ Upgrade multiple databases in the same Oracle Home. ▪ Upgrade multiple databases across Oracle Homes on the same host. ▪ Upgrade multiple databases on different hosts. <p>You can even upgrade onedatabase instance at a time. For example, if you have already upgraded some of the databases in the Oracle home earlier, and you now want to upgrade the other databases in the same Oracle home.</p> <p>Oracle RAC Database</p> <p>You can upgrade only one Oracle RAC database instance at a time. mass upgrade is not supported at the moment.</p>	<p>To mass upgrade single instance databases, see Section 14.4.</p> <p>To upgrade one single instance database or one Oracle RAC database instance, see Section 14.5.</p>
Step 2	<p>Knowing About the Supported Releases</p> <p>Know what releases of Oracle Database can be upgraded by the Deployment Procedure.</p>	<p>To learn about the releases supported by the Deployment Procedure, see Section 14.2.</p>
Step 3	<p>Understanding the Deployment Procedure</p> <p>Understand the Deployment Procedure you need to select, and its scope and coverage.</p>	<p>To learn about the Deployment Procedure offered for upgrading databases, see Section 14.3.</p>
Step 4	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	<ul style="list-style-type: none"> ▪ To learn about the prerequisites for mass upgrade of Oracle Databases, see Section 14.4.1. ▪ To learn about the deployment phases involved in upgrading a database instance, see Section 14.5.1.
Step 5	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully upgrade Oracle database.</p>	<ul style="list-style-type: none"> ▪ To learn about the procedure for mass upgrade of Oracle Databases, follow the steps explained in Section 14.4.2. ▪ To learn about the procedure to upgrade a database instance, see Section 14.5.2.

14.2 Supported Releases

Using this Deployment Procedure, you can mass upgrade the following releases of Oracle Database across multiple hosts:

Table 14–2 Supported Releases for Mass Upgrade of Oracle Databases

Supported Target	Supported Release to Upgrade to	Supported Platform
Oracle Database (single instance database)	11g Release 2	All Platforms

For upgrading one database instance, the following releases are supported:

Table 14–3 Supported Releases for Upgrading a Database Instance

Supported Target	Supported Release to Upgrade to	Supported Platform
Oracle Database (single instance database)	11g Release 2	All Platforms
Oracle Real Application Clusters (Oracle RAC)	11g Release 2	All Platforms
Oracle RAC One	11g Release 2	All Platforms

14.3 Deployment Procedure

Cloud Control offers the *Upgrade Oracle Database* deployment procedure for mass upgrade of Oracle databases. The deployment procedure supports the following usecases:

- Upgrade of multiple databases in the same Oracle Home
- Upgrade of multiple databases across Oracle Homes on the same host
- Upgrade of multiple databases on different hosts

For upgrading one Oracle database instance at a time or any Oracle RAC database instance, you must access the Oracle Database Upgrade wizard from the Home page of the database that you want to upgrade.

Note: The Upgrade Database deployment procedure does not support upgrade of databases in Oracle Data Guard configurations and databases with Oracle Database Vault.

The Deployment Procedure can be run by two types of administrators, mainly Designer and Operator. As a designer, you can set up a test database, deploy new software and patches, and test the upgrade process, and then create a gold image out of it. You can then access the Deployment Procedure, provide the required details, and lock one or more of the fields, such as platform, version, move to, and so on. Finally, you can save the procedure and then publish it to the operators.

As an operator, you can access the save procedure and perform only certain operations such as selecting a set of databases based on the locked criteria, providing any additional input that is specific to the runtime activity, and then scheduling the procedure. This way, the operators run a fully tested and certified Deployment Procedure in their production environments, and the entire operation tends to be less error prone.

For more information on these types of administrators, and to learn how you can use these locking feature, see [Section 2.4](#).

14.4 Upgrading Multiple Oracle Database Instances at a Time (Mass Upgrade)

This section describes how you can perform mass upgrade of single-instance databases.

Note: Mass upgrade of Oracle RAC database is not supported at the moment, so Oracle recommends that you use the wizard described in [Section 14.5](#) to upgrade one Oracle RAC database instance at a time.

This section covers the following:

- [Prerequisites](#)
- [Upgrade Procedure](#)

14.4.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites.

- To upgrade to 11.2.0.x, the existing database version must be 10.2.0.4 or higher, 11.1.0.6 or higher, or 11.2.0.1. Make sure the target version (that is, the version you are upgrading to) is always higher than the source version.
- Database user must have SYSDBA privileges or the OS user must be part of the DBA group.
- Database to be upgraded must be up and running.
- Ensure that you have created designer and operator roles with the requisite privileges. The designer must have EM_PROVISIONING_DESIGNER role and the operator must have EM_PROVISIONING_OPERATOR role.

Prerequisites for Designers

- Edit access to Software Library to manage Software Library entities such as gold images
- Add/Edit Target privileges
- Create Named Credentials privilege

Prerequisites for Operators

- View access to Software Library to view Software Library entities such as gold images.
- Add/View Target privileges.
- Privileges to the named credentials granted by designer.

14.4.2 Upgrade Procedure

Follow these steps:

1. Log in as a designer, and from the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.

2. In the Database Provisioning console, select the **Upgrade Oracle Database** Deployment Procedure and click **Launch**. The Oracle Database Upgrade wizard is launched.
3. In the Select Databases page, select the databases to be upgraded. You can select:
 - Multiple databases in the same Oracle Home
 - Multiple databases across Oracle Homes on the same host
 - Multiple databases on different hosts

In the Select Databases section, select the **Platform** and **Version** of the database to be upgraded. You can search for database, host, target group, or Oracle Home and then select the database.

Click **Schedule Backup** to schedule a backup of the database. If you do not back up your databases before upgrade, you may not be able to restore the databases if upgrade fails.

Note: If the database you want to upgrade does not appear in the table, verify that the database is available and there are no metrics collection errors for the target.

In the Select Upgrade Path section, select the version you want to **Move to**. The upgrade version selected must be higher than the present version of the database. You can move to the latest database release available.

Click on the Lock icon to lock the fields that you do not want to be editable. These fields will not be available for editing in the operator role. For example, locking **Platform** and **Version** fields will ensure that the operator selects databases from the specific list of platform and version for the upgrade.

Click **Next**.

4. In the Specify Path details page, select Upgrade Option as one of the following:
 - Select **Upgrade Database Software and Instance** to install a new Oracle Home and upgrade the database instance. Specify the following details:
 - a. In the Oracle Database Software Details section, select the **Oracle Database Software** from the Software Library for installing a new Oracle Home. Ensure that the zipped up Oracle Home contains all critical patches for the new Oracle Home.

Note: To ensure that the gold image you create includes all the recommended patches, follow these steps:

1. Click the 'Database Upgrade Planner' link and Log in to My Oracle Support using Cloud Control in the online mode.
 2. Select the following types of patches to be applied to the gold image:
 - Recommended patches on the release you want to upgrade to
 - Patches on top of the release that maintain the fixes in the base release
 - Patches resolving merge conflicts if any present between the patches chosen
 3. Apply the patches to an Oracle Home of the release to upgrade to using Patch Plans or manually. For more information about patch plans, see [Chapter 24](#).
 4. Create a gold image from the Oracle Home and use it for the upgrade. For information about creating a gold image, see [Section 4.3.9](#).
-
-

- b. In the Specify New Software Location section, specify the **Oracle Home** and **Oracle Base** to upgrade the database. Select **Same for all hosts** to upgrade all databases from a host to the same Oracle Home by specifying the same Oracle home location.
 - c. In the Advanced section, specify the **Working Directory** for the upgrade. Ensure that you have read-write permissions to this directory.
- Select **Upgrade Database Instance Only** to upgrade the database instances in an existing Oracle Home. For example, if you have already upgraded some of the databases in the Oracle Home earlier and want to now upgrade other databases in the same Oracle Home. Specify the following:
 - a. In the Select an existing location for Database Instance section, specify the **Oracle Home** on the host where you want to upgrade the database.

Click on the Lock icon to lock the fields that you do not want to be editable. These fields will not be available for editing in the operator role.

Click **Next**.

5. In the Specify Configuration Details page, you can configure the listener to be registered with the database after upgrade as follows:
 - Use an existing listener. The databases after upgrade, will be registered automatically with the Single Instance High Availability listener, if configured. If no Single Instance High Availability listener is available, and there are other listeners running in the Oracle Home, the upgraded databases will be registered with these listeners.
 - Add a new listener.

If you are upgrading multiple databases in the same Oracle Home, you can use the same listener for these databases.

Note: Migration of existing listeners is not supported.

In the Listener Configuration section, click the plus sign (+) to select listener for the database. In the Select Listener for Database popup:

- a. Select the listener if it already exists. Otherwise, click **Add** to add a new listener to register with the database. Specify the **Name** and **Port**.
- b. Click **OK**.

In the Backup and Restore section, you can select:

- **Backup and Restore Settings Only** to restore configuration changes made during database upgrade and not actual data, in case upgrade fails.
- **Full Backup** to backup the database and restore configuration and oratab settings if upgrade fails. The backup location is, by default, \$ORACLE_BASE/admin/\$GDB/backup where '\$GDB' is the global database name.
- **Ignore** if you have your own backup options and do not want Cloud Control to perform a backup of your database.

In the Upgrade Options section:

- Select **Recompile invalid objects at the end of upgrade** to make valid database objects for the new database version.
- If archive logging has been turned on for the database, then you have the option to **Turn off Archiving and flashback logging, for the duration of upgrade**.
- If you are upgrading to database version 11.2.0.2 or higher, you will be able to set the time zone upgrade option. You can select **Upgrade Time Zone Version and Timestamp with Time Zone data**.

In the Advanced section, select custom scripts to run on the database before or after upgrade. Select **Execute custom SQL script on the source database before upgrading the database** to run custom script on the database before upgrade and then select the script from the Software Library. Select **Execute custom SQL script on the upgraded database** to run custom script on the upgraded database and then select the script from the Software Library.

Click on the Lock icon to lock the fields that you do not want to be editable. These fields will not be available for editing in the operator role.

Click **Next**.

6. The Custom Properties page will be displayed only for user customized deployment procedures that require custom parameters. Specify custom properties for the upgrade, if any. Click **Next**.
7. In the Select Credentials page, specify the Operating System, Privileged Operating System Credentials (run as root), and Database credentials. If you choose to specify Preferred Credentials, select either Normal Host or Privileged Host credentials. For Named Credentials, you can specify the same or different credentials for Oracle homes.

If you have not set Named Credentials, click the plus sign (+) in the Credentials section. In the Add New Database Credentials popup, specify the **User name**, **Password**, **Role**, and specify the Save Details. Select **Run As** and specify **root**. Click **OK**.

Click on the Lock icon to lock the fields that you do not want to be editable. These fields will not be available for editing in the operator role.

Click **Next**.

8. In the Schedule page, specify a **Deployment Instance** and schedule for the upgrade job. If you want to run the procedure immediately, then retain the default selection, that is, Immediately. If you want to run the job later, then select Later and provide time zone, start date, and start time details. Specify a Grace Period, a duration after the start period for Cloud Control to attempt to start the upgrade if it cannot start at the specified time.

In the Set Breakpoint section, configure to continue or stop the deployment procedure execution after each step is run. For example, if you set the breakpoint after analyzing the prerequisites, the upgrade will pause after the prerequisites are run. You can verify that the prerequisites have run successfully, fix any errors, and then run the upgrade.

In the Set Notification Details section, select the events for which you want to be notified.

Click **Next**.

9. In the Review page, verify that the details you have selected are correctly displayed. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes.

To save the deployment procedure for future use, click **Save**.

To submit the deployment procedure, click **Submit**. When the deployment procedure is submitted for execution, the database upgrade instance tracking page is displayed. You can also navigate to this page by clicking the procedure instance in the Job Activity page.

10. You can run the saved deployment procedure as an Cloud Control user with operator role by selecting the configured and saved Database Upgrade Deployment Procedure instance in the Database Provisioning console, and clicking **Launch**.
11. Submit the configured Database Upgrade procedure after providing values for the editable fields. After you have submitted the procedure, the summary for the running procedure is displayed.
12. In the Upgrade Oracle Database procedure execution page, in the Current Run tab, view the upgrade job steps and status.
13. If you have specified a breakpoint, the procedure execution will pause at the step specified. From the **Actions** menu, select **Resume**. The possible actions are Stop, Resume, Suspend, Cleanup, Resubmit, and Skip Step. Click **Resubmit** to resubmit the current instance for execution.
14. If you want to execute certain steps, from the **Run to step** list, select the step you want to run.
15. If a step has status Failed, click **View Log**. The Job Run for the step is listed. Click **Show** in the Details column to view the entire log. Fix the error and click **Retry**.
16. After the procedure execution is completed, click on the **Targets** menu and select **All Targets** to navigate to the All Targets page and verify that the newly upgraded databases appear as Cloud Control targets.

14.5 Upgrading One Oracle Database or One Oracle RAC Database Instance at a Time

This section describes how you can use the wizard to upgrade one single instance database or one Oracle RAC database instance at a time.

Note: Since mass upgrade of Oracle RAC database is not supported at the moment, Oracle recommends that you use the wizard described in this section to upgrade one Oracle RAC database instance at a time.

Note: To upgrade one single instance database or one Oracle RAC database instance at a time, from the respective database home page, from the target menu, select **Provisioning**, then select **Upgrade Database**.

For single instance database instances, you will see another menu option to upgrade the Oracle home and the instance. If you select that option, you will be taken to the wizard described in [Section 14.4](#), however, only the database instance, from where you navigated to the wizard, will be pre-selected for upgraded.

This section covers the following:

- [Prerequisites](#)
- [Upgrade Procedure](#)

14.5.1 Prerequisites

- The database version must be 10.2.0.4 or above for upgrade to 11.2.0.1 or higher.
- For Oracle Real Application Clusters databases, if you select an Oracle RAC database instance and start the database upgrade process, it will upgrade the entire cluster database.
- If OS authentication is not turned on, SYSDBA credentials are required for the upgrade.
- Database to be upgraded must be up and running.
- Ensure that you have DBA privileges to run this procedure.

14.5.2 Upgrade Procedure

Follow these steps:

1. From the **Enterprise** menu, select **Targets**, then select **Database**. In the Databases page, select the source database to be upgraded.
2. In the Database Instance home page, from the **Oracle Database** menu, select **Provisioning**, then select **Upgrade Database**.

Note: For single instance database instances, you will see another menu option to upgrade the Oracle home and the instance. If you select that option, you will be taken to the wizard described in [Section 14.4](#), however, only the database instance, from where you navigated to the wizard, will be pre-selected for upgraded.

3. Specify the Database user and password credentials and click **Continue**. The Database Upgrade wizard is launched.

4. In the Oracle Home page, select the **New Oracle Home** where you want the new Oracle Home for the upgrade to be installed, based on the version of the database to be upgraded. If the Oracle Home is not a discovered target in Cloud Control, either discover the Oracle Home using the Cloud Control Discovery feature and then initiate the upgrade process or type the path of the Oracle Home manually. For Oracle Real Application Clusters databases, specify the Oracle RAC home.

For information about discovering targets in Cloud Control, see [Chapter 3](#).

When specifying the new Oracle Home, you must have DBA permissions on both the source and destination Oracle Homes and these Oracle Homes must reside on the same host.

In the Oracle Home Credentials section, specify the host credentials. Host credentials must have DBA privileges and can be **Preferred Credentials**, or **Named Credentials**, or you can select **Enter Credentials** and specify the user name and password and save it. Click **More Details** to view details about the host credentials you have selected. The specified Oracle Home credentials should have privileges on both the source database Oracle Home and the new Oracle Home. Click **Test** to verify that the credentials have the required privileges. If you are using Named Credentials, ensure that these are user and password credentials, else they will not be supported in Cloud Control.

Click **Next**. The errors and warnings from the prerequisite checks are displayed. Fix all errors and warnings and revalidate. Click **OK** to proceed to next step.

5. In the Options page, the Diagnostics destination field is displayed only for database upgrade from version 10.2.x to 11.1.0.6. The diagnostic destination is defaulted to Oracle Base and all diagnostic and trace files are stored at this location.

If you are upgrading from version 11.1.0.7 or higher to 11.2.x, the diagnostic destination field does not appear.

If archive logging has been turned on for the database, then you have the option to disable or **Keep archive logging enabled during upgrade**.

If flash recovery area has been configured for the database, then the Flash Recovery section will be displayed. Specify **Flash Recovery Area Location** and provide an adequate space for **Size**.

If you are upgrading to database version 11.2.0.2 or higher, you will be able to set the time zone upgrade option. You can select to **Upgrade Time Zone Version and Timestamp with Time Zone data**.

Note: If the database has ASM configured with it, the Backup section will not be displayed.

In the Backup section, you can select:

- **Restore Settings Only** to restore configuration changes made during database upgrade and not actual data, in case upgrade fails.
- **Perform full backup before upgrade and restore upon failure** to restore oratab configuration. Specify a file system location for **Backup Location**. The credentials that you have specified earlier must have read-write permissions to this location.
- **None** if you do not want to specify a database backup.

In the Advanced section, specify the custom SQL scripts you want to run before and after the database upgrade. Copy these scripts to the host file system and select them. If your custom scripts are stored as a component in the Software Library, select **Select these scripts from the Software Library** and then browse the Software Library for these scripts. During execution, the main file specified in the Software Library component will be run. So, if you want to run a set of scripts, organize them in the main script file and specify the main script in the Software Library component.

Select **Recompile invalid objects at the end of upgrade** to make valid database objects for the new database version. Setting a higher **Degree of Parallelism** will ensure faster recompilation of objects. The default setting is the number of CPU count of the host.

Click **Next**.

6. The Listeners page is displayed only for single instance database upgrade. In the Listeners page, listeners that are registered with Oracle Restart and those that are running in the new Oracle Home are displayed. You can create a new listener or migrate your existing listener manually and then upgrade the database. If you create a new listener, the listener will then be an Cloud Control target and will be monitored. If you migrate your existing listener, the upgrade job will register the database with the listener.

If you have listeners running in the source Oracle Home and need to maintain the same listener port after upgrade, migrate your listener manually to the new Oracle Home first.

For Oracle Real Application Clusters database, the upgraded database will be registered with the Clusterware listener automatically and the Listeners page will not appear.

To add a new listener, specify the **Name** and **Port Number**.

Click **Next**.

7. In the Schedule page, edit or retain the Job **Name** and **Description** for the database upgrade. If you want to run the job immediately, then retain the default selection, that is, Immediately. If you want to run the job later, then select Later and provide time zone, start date, and start time details. Specify a Grace Period, a duration after the start period for Cloud Control to attempt to start the upgrade job if it cannot start at the specified time.

Select **Blackout the database target in Enterprise Manager during upgrade** if you do not want the database to be monitored and alerts to be raised by Cloud Control during the upgrade.

Click **Next**.

8. In the Review page, ensure that you review all warnings generated in the Validation Summary. Click the Validation Summary icon to view validation results and severity and action taken for any warnings. Verify that the details you have provided for the upgrade job appear correctly and then click **Submit Job** to run the job according to the schedule set. If you want to modify the details, then click **Back** repeatedly to reach the page where you want to make the changes. Click **Save** to save the deployment procedure for future deployment.
9. After you have submitted the job, the Database Upgrade Job page with the summary for the running job will be displayed. In the Jobs page, view the job summary and the list of steps and view their status.

10. After the upgrade job is completed successfully, click on the **Targets** menu and select **All Targets** to navigate to the All Targets page and verify that the newly upgraded database is displayed as an Cloud Control target with the correct database version.

Part V

Middleware Provisioning

This part contains the following chapters:

- [Chapter 15, "Provisioning WebLogic Domains and Middleware Homes"](#)
- [Chapter 16, "Scaling Up / Scaling Out WebLogic Domains"](#)
- [Chapter 17, "Deploying / Redeploying / Undeploying Java EE Applications"](#)
- [Chapter 18, "Provisioning Coherence Nodes and Clusters"](#)
- [Chapter 19, "Provisioning SOA Artifacts and Composites"](#)
- [Chapter 20, "Provisioning Oracle Service Bus Resources"](#)
- [Chapter 21, "Provisioning Oracle BPEL Processes"](#)
- [Chapter 22, "Provisioning Oracle Application Server"](#)

Provisioning WebLogic Domains and Middleware Homes

This chapter explains how you can automate common provisioning operations for Middleware Homes and WebLogic Domains using Oracle Enterprise Manager Cloud Control. It covers the following:

- [Getting Started](#)
- [Middleware Provisioning Deployment Procedures](#)
- [Prerequisites for Designers and Operators](#)
- [Creating Software Library Components](#)
- [Cloning from an Existing Installation](#)
- [Cloning from a Profile or a Middleware Home Gold Image](#)
- [Post Deployment Configuration](#)
- [Customizing the Deployment Procedure](#)

15.1 Getting Started

This chapter helps you get started by providing an overview of the steps involved in provisioning WebLogic Domains and Middleware Homes. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision a WebLogic domain. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 15–1 *Getting Started with Provisioning a WebLogic Domain or a Middleware Home*

Step	Description	Reference Links
Step 1	<p>Understanding the Deployment Procedure</p> <p>Understand the Deployment Procedures offered by Cloud Control for provisioning WebLogic Domains and Middleware Homes. Know how the Deployment Procedure functions, what use cases it covers, and so on.</p>	To learn about the Deployment Procedures, see Section 15.2 .

Table 15–1 (Cont.) Getting Started with Provisioning a WebLogic Domain or a Middleware Home

Step	Description	Reference Links
Step 2	<p>Knowing About the Supported Releases</p> <p>Know what releases can be provisioned by the Deployment Procedure.</p>	To learn about the releases supported by the Deployment Procedure, see Section 15.3 .
Step 3	<p>Selecting the Use Case</p> <p>This chapter covers the use cases for provisioning a WebLogic Domain and a Middleware Home. Select the use case that best matches your requirement.</p>	<ul style="list-style-type: none"> ■ To create a component in the Software Library for a WebLogic Domain and its Middleware Home (to be used as the source for future cloning operations), see Section 15.5.1. ■ To create a component in the Software Library for a Middleware Home and its binaries (to be used as a source for future cloning operations), see Section 15.5.2. ■ To provision WebLogic binaries and domain configuration from an existing installation, see Section 15.6.1. ■ To provision binaries from an existing installation's Middleware Home, see Section 15.6.2. ■ To provision WebLogic binaries and domain configuration from a profile already created in the Software Library, see Section 15.7.1. ■ To provision a Middleware Home and its binaries from a gold image already created in the Software Library, see Section 15.7.2.
Step 4	<p>Meeting the Prerequisites</p> <p>Before you create a component in the Software Library or any Deployment Procedure, you must meet the prerequisites, such as space requirements and user privileges. When you run the Deployment Procedure, these prerequisites are verified.</p>	<ul style="list-style-type: none"> ■ To learn about the prerequisites for creating a WebLogic Domain Provisioning Profile, see Section 15.5.1. ■ To learn about the prerequisites for creating a Oracle Middleware Home Gold Image, see Section 15.5.2. ■ To learn about the prerequisites for cloning a WebLogic Domain from an existing installation, see Section 15.6.1.1. ■ To learn about the prerequisites for cloning a Middleware Home from an existing installation, see Section 15.6.2.1. ■ To learn about the prerequisites for cloning a WebLogic Domain from a domain provisioning profile, see Section 15.7.1.1. ■ To learn about the prerequisites for cloning a Middleware Home from an Oracle Middleware Home gold image, see Section 15.7.2.1.

Table 15–1 (Cont.) Getting Started with Provisioning a WebLogic Domain or a Middleware Home

Step	Description	Reference Links
Step 5	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully provision a Middleware Home or a WebLogic Domain.</p>	<ul style="list-style-type: none"> ■ To clone WebLogic domains and domain configuration from an existing installation, follow the steps explained in Section 15.6.1.2. ■ To clone binaries from an existing installation's Middleware Home, follow the steps explained in Section 15.6.2.2. ■ To clone WebLogic binaries and domain configuration from a profile already created in the Software Library, follow the steps explained in Section 15.7.1.2. ■ To clone a Middleware Home and its binaries from an Oracle Middleware Home Gold Image already created in the Software Library, follow the steps explained in Section 15.7.2.2.

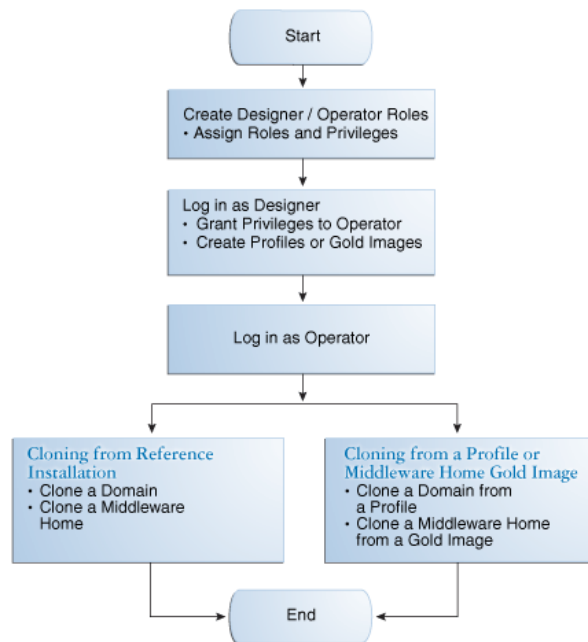
15.2 Middleware Provisioning Deployment Procedures

Using the Middleware Provisioning deployment procedures, you can clone a WebLogic Domain and /or a Middleware Home. This section covers the following:

- [Cloning from an Existing Installation](#)
 - [Cloning a WebLogic Domain from an Existing Installation](#)
 - [Cloning a Middleware Home from an Existing Installation](#)
- [Cloning from a Profile or a Middleware Home Gold Image](#)
 - [Cloning from a WebLogic Domain Provisioning Profile](#)
 - [Cloning from an Oracle Middleware Home Gold Image](#)

Before you run these deployment procedures, you must have created the profile or the gold image in the Software Library. See [Section 15.5](#) for details.

The following figure shows the sequence of operations involved in cloning a WebLogic Domain or a Middleware Home.

Figure 15–1 Cloning a WebLogic Domain or a Middleware Home

- Cloning from a Reference Installation: See [Figure 15–4](#).
- Cloning from a Profile or a Software Library component.
 - To clone from a provisioning profile, see [Figure 15–10](#).
 - To clone from a Software Library component, see [Figure 15–11](#).

15.3 Supported Releases

Cloud Control supports Oracle WebLogic Server versions 10.3.1.0, 10.3.2.0, 10.3.3.0, 10.3.4.0, 10.3.5.0, 10.3.6.0, and 12.1.1.

15.4 Prerequisites for Designers and Operators

This section describes the prerequisites required by Designer and Operator users before the Middleware Provisioning deployment procedures can be executed. It contains the following sections:

- [Prerequisites for Designers](#)
- [Prerequisites for Operators](#)
- [Additional Prerequisites on Windows](#)

15.4.1 Prerequisites for Designers

Designers are lead administrators with increased privileges on Deployment Procedures and Software Library. For more details, see *Overview of User Accounts*.

Following are the prerequisites required for designers to create components in the library, customize the deployment procedure, and create and save deployment procedures for future usage by operators.

- Ensure that you meet the infrastructure requirements described in [Chapter 2](#).
- Discover and monitor the destination hosts in Cloud Control. For this purpose, you need the latest version of Oracle Management Agent (Management Agent) on the destination hosts. For more information refer to the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. Ensure that the agents are installed in the same location on all hosts.
- Set up the Oracle Software Library (Software Library). Create a folder to store the Software Library components and add components to the folder. Ensure that the WebLogic Domain Provisioning Profile and the Middleware Home Gold Image components have been added to the folder. For information about creating them, see [Section 15.5](#).
- Store the operating system credentials of the destination hosts as preferred credentials in Oracle Management Repository (Management Repository) or use Named Credentials.

If you are using SUDO, PowerBroker, see [Section 2.3.3](#) for information on setting up these authentication utilities.
- You must have **Write** permissions on the following locations:
 - Oracle base directory for Grid Infrastructure where diagnostic data files related to Grid Infrastructure can be stored.
 - Grid Infrastructure software directory where Grid Infrastructure software can be provisioned.
- You must have **Operator** target privileges on the destination host machines.

15.4.2 Prerequisites for Operators

Operators are administrators who have restricted privileges on a Deployment Procedure and Software Library. Normally, operators can view and submit a deployment procedure. The Designer user may also grant the Operator the necessary privileges on any targets or entities. For more details, see *Overview of User Accounts*.

Following are the prerequisites for operators who will run the deployment procedures:

- You must have permissions to view credentials (set and locked by the designer), view targets, submit jobs, and launch deployment procedures.
- You must have **Operator** target privileges in the destination host machines.
- If you are cloning a WebLogic domain using an existing installation, you must have Write access to the directory location of the Middleware Home or the WebLogic domain on the destination host machine.
- If you are using an external JDK, ensure that the JDK software has been installed on the destination host before you launch the deployment procedure.
- Middleware Home Requirements:
 - **Existing Middleware Home:** The Middleware Home on the destination machine must be identical in content and product stack as the Middleware Home on the source machine.
 - **Create New Middleware Home:** Ensure that there is sufficient disk space on the destination machine. The space required is approximately 2 times the size of the source Middleware Home.

- **Shared Middleware Home:** This option is applicable when you are provisioning on multiple hosts. You must specify an absolute shared mount directory that is accessible by all destination hosts.

15.4.3 Additional Prerequisites on Windows

Following are the additional prerequisites required when you run the deployment procedures on Windows:

- The Operating System user must be part of the Administrators Group.
- If the source Middleware Home is being cloned, ensure that the Node Manager service has been stopped.
- Ensure that directory paths and locations you specify are in the Windows standard format.

15.5 Creating Software Library Components

If you are using a profile or a gold image to provision your WebLogic Domain or Middleware Home, you must create the necessary components in the Software Library. This section describes the procedures to create these components. It covers the following:

- [Creating a WebLogic Domain Provisioning Profile](#)
- [Creating an Oracle Middleware Home Gold Image](#)

15.5.1 Creating a WebLogic Domain Provisioning Profile

A WebLogic Domain Provisioning Profile consists of the Middleware Home, binaries and the domain configuration. You can create a profile, save it in the Software Library, and then use the saved profile as the source for creating new WebLogic domains. This will ensure that future WebLogic installations follow a standard, consistent configuration.

Prerequisites

- The Management Agent must be running on the Administration Server.
- You must have the host credentials for the Administration Server running on the source machine.
- The WebLogic domain for which the profile is being created must be a monitored target in Cloud Control.
- The disk space required to create a profile is calculated as follows:

Disk Space = Middleware Home Size + WebLogic Domain Size + Space for Temporary Scripts

To create an Oracle Middleware Profile, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. From the **Actions** menu, click **Create Folder** to create a folder in which the profile you are creating is to be stored. We recommend that you do not use an out-of-box folder to store the profile.
3. Select the folder that you have created, and from the **Actions** menu, select **Create Entity**, and then **Component**.

4. A Create Component popup window appears. From the Select Subtype drop-down list, select the **WebLogic Domain Provisioning Profile** component and click **Continue**.
5. In the Create WebLogic Domain Provisioning Profile: Describe page, the Parent Directory under which the profile will be created and the Subtype are displayed. Enter a name (only alphanumeric characters and underscores are allowed) and description for the profile and enter the values for the Product Version, Product, and Vendor attributes. For example, enter the Product Version as 10.3.3, Product as WebLogic Domain, and Vendor as Oracle.
6. Click **Next**. The Create WebLogic Domain Provisioning Profile: Configure page appears.

Figure 15–2 Create WebLogic Domain Provisioning Profile: Configure

The screenshot shows the 'Configure' step of creating a WebLogic Domain Provisioning Profile. The 'WebLogic Domain' is set to 'GCDomain' and the 'Host' is 'slc0Dejc.us.oracle.com'. The 'Working Directory' is '/tmp/fmwProvSrc'. The 'Source Information' section contains the following table:

Component	Location
GCDomain	/scratch/aimc/MW_120718/gc_inst/user_projects/domains/GCDomain
Middleware Home	/scratch/aimc/MW_120718
WebLogic Server 10.3	/scratch/aimc/MW_120718/wlserver_10.3
Oracle Home(s)	
oms	/scratch/aimc/MW_120718/oms

The 'Host Credentials' section shows 'Named' as the selected credential type. The 'Credential Name' is 'CS_ALL'. The 'Credential Details' table is as follows:

Attribute	Value
UserName	aimc
Password	*****

7. Click the **Search** icon next to the WebLogic Domain field and select a WebLogic Domain from which the profile is to be created. The profile will include both the software in the Middleware Home as well as the configuration in the WebLogic Domain home.

Note: To upload a profile without binaries, deselect the **Include the binaries from the Middleware Home in the profile to be created** checkbox. If you select a profile without binaries, during provisioning, you must select an existing Middleware Home that is the same version as the one selected in the source installation.

8. In the Working Directory field, specify the directory on the host machine on which the files required for creating the profile are temporarily stored. If this directory is not present, it will be created. When the profile has been created, the contents of this directory will be deleted.
9. In the Host Credentials section, enter the host credentials of the machine on which the Administration Server of the source WebLogic Domain is installed. Select one of the following options:

- **Preferred Credentials:** The preferred credentials stored in the Management Repository are used. The Preferred Credentials option will be available only if it has already been defined in Cloud Control. For more information on setting up Preferred Credentials, see Managing Preferred Credentials.
 - **Named Credentials:** The credentials stored in the Management Repository is used. To use the Named Credentials stored in the Management Repository, you must have already registered each of the preferred credential types with a unique name. Select the desired Named credential from the list available in Credential Name. For more information on registering a name for the preferred credentials, see Managing Named Credentials.
 - **New Credentials:** You can override the preferred credentials by specifying a new credential with a unique name and password.
10. Click **Next**. In the Review page, you can review the information and click **Save and Upload**.
 11. The Job Name is displayed at the top of the page. Navigate to the Job Activity page and check the job status. Once it has been completed, navigate to the Software Library page and confirm if all the components of the profile (WebLogic Domain, MWHome, and Profile) have a **Ready** Status. You can also verify if the profile has been successfully created by navigating to the Middleware Provisioning page. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning** and check if the profile is displayed there. You can now use this profile as the source for future WebLogic Domain installations.

15.5.2 Creating an Oracle Middleware Home Gold Image

You can create an Oracle Middleware Home Gold Image and save it in the Software Library. You can then use this gold image as the source for future Middleware Home installations.

Prerequisites

- The Management Agent must be running on the Administration Server.
 - You must have the host credentials for the Administration Server running on the source machine.
 - The disk space required to create a gold image is calculated as follows:
Disk Space = Middleware Home Size + Space for Temporary Scripts
1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
 2. From the **Actions** menu, click **Create Folder** to create a folder in which the gold image you are creating is to be stored. We recommend that you do not use an out-of-box folder to store the gold image.
 3. Select the folder you have created and from the **Actions** menu, select **Create Entity**, then select **Component**.
 4. A Create Component popup window appears. From the Select Subtype drop-down list, select the Oracle Middleware Home Gold Image component and click **Continue**.
 5. In the Describe page, the Parent Directory under which the gold image will be created and the Subtype are displayed. Enter a name and description for the profile and enter the values for the Product Version, Product, and Vendor

attributes. For example, enter the Product Version as 10.3.3, Product as Middleware Home, and Vendor as Oracle.

6. Click **Next**. Create Oracle Middleware Home Gold Image: Configure page appears. Click the **Search** icon next to the Middleware Home field and select an existing Middleware Home from which the gold image is to be created.

Figure 15–3 Create Oracle Middleware Home Gold Image: Configure

The screenshot shows the 'Create Oracle Middleware Home Gold Image: Configure' page. At the top, there are navigation buttons: 'Describe', 'Configure' (active), and 'Review'. Below this, the title 'Create Oracle Middleware Home Gold Image : Configure' is displayed, along with 'Step 2 of 3' and buttons for 'Back', 'Next', 'Save', and 'Cancel'. The page indicates the 'Parent Directory' is 'FPMW Profiles' and the 'Subtype' is 'Oracle Middleware Home Gold Image'. A note states: 'In order to create a Oracle Middleware Home Gold Image, you must first select an existing Middleware Home. The home selected would be archived and stored in the software library for future cloning operations.' Below this, a search bar shows 'Middleware Home /scratch/sheyang/mwh_ps4' with a magnifying glass icon. The 'Host' is 'adc2190523.us.oracle.com' and the 'Working Directory' is '/tmp/fmwProvSrc'. The 'Source Information' section contains a table:

Component	Location
Middleware Home	/scratch/sheyang/mwh_ps4
WebLogic Server 10.3	/scratch/sheyang/mwh_ps4/wlserver_10.3

The 'Host Credentials' section includes a note: 'If you choose Preferred Credentials, the job will use your preferred credentials for each target at the time job runs, and therefore requires credentials for all targets to be set. If you choose to override the preferred credentials, one set of credentials will be used for all targets of each type.' There are three radio buttons: 'Preferred' (selected), 'Named', and 'New'. The 'Preferred Credential Name' is 'Normal Host Credentials'. A 'Credential Details' table is shown below:

Attribute	Value
UserName	sheyang
Password	*****

A 'More Details' link is located below the table.

7. In the Working Directory field, specify the directory on the destination Host on which the files required for creating the gold image are temporarily stored. If this directory is not present, it will be created. When the gold image has been created, the contents of this directory will be deleted.
8. In the Host Credentials section, enter the host credentials of the machine on which the Middleware Home is located. Select one of the following options:
 - **Preferred Credentials:** The preferred credentials stored in the Management Repository are used. The Preferred Credentials option will be available only if it has already been defined in Cloud Control.
 - **Named Credentials:** The credentials stored in the Management Repository is used. To use the Named Credentials stored in the Management Repository, you must have already registered each of the preferred credential types with a unique name. Select the desired Named credential from the list available in Credential Name.
 - **New Credentials:** You can override the preferred credentials by specifying a new credential with a unique name and password. These credentials can be different for each host or the same for all the hosts.
9. Click **Next**.- In the Review page, you can review the information and click **Save and Upload**.
10. The Job Name is displayed at the top of the page. Navigate to the Job Activity page and check the job status. Once it has been completed, navigate to the Software Library page and confirm if all the components of the gold image have a Ready Status. You can also verify if the gold image has been successfully created

by navigating to the Middleware Provisioning page. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning** and check if the gold image is displayed there. You can now use this gold image for future cloning operations.

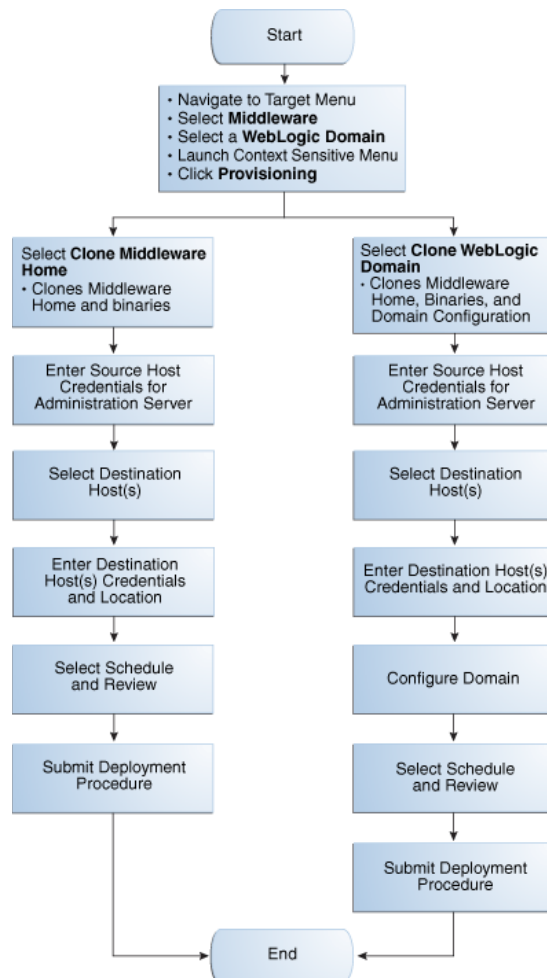
15.6 Cloning from an Existing Installation

This section describes the procedures to clone a WebLogic Domain or a Middleware Home from an existing installation. It contains the following sections:

- [Cloning a WebLogic Domain from an Existing Installation](#)
- [Cloning a Middleware Home from an Existing Installation](#)

Figure 15–4 shows the sequence of operations involved in cloning a WebLogic Domain or a Middleware Home from an existing installation.

Figure 15–4 Cloning from an Existing Installation



15.6.1 Cloning a WebLogic Domain from an Existing Installation

This section describes the procedures used to clone a WebLogic Domain from an existing installation. It covers the following:

- [Prerequisites](#)
- [Deployment Procedure](#)

15.6.1.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

- The destination host machines on which the Middleware domains are to be cloned must be discovered targets in Cloud Control.
- The Operating System Host user must have Read permissions on:
 - Middleware directory on the host machine on which the Administration Server is running.
 - Administration Server host domain directory.
 - Agent home directory.
- The user must have Write permissions on:
 - Working Directory on the source host machine which Administration Server is running.
 - Working Directory on all destination hosts.
 - Middleware Home directory on all destination hosts.
 - Domain location on all destination hosts
- The ports on the Administration Server, Managed Server, and Node Manager on the destination host must be free.

15.6.1.2 Deployment Procedure

The **Clone WebLogic Domain** option launches a wizard that enables you to clone a WebLogic Domain from an existing reference domain that is already discovered with Cloud Control. It allows you to clone the Middleware Home and its binaries, and the domain configuration.

To clone a WebLogic Domain from an existing installation, follow these steps:

1. From the **Targets** menu, select **Middleware**.
2. A list of Middleware targets is displayed. Find the WebLogic Domain that you want to use as the source for the cloning operation. Right click on that WebLogic Domain to access the context sensitive menu and select the Provisioning menu option. From the menu, select **Provisioning** and **Clone WebLogic Domain**.
3. You can select:
 - **Clone Middleware Home:** Select this option if you want to clone only the software in the Middleware Home.
 - **Clone WebLogic Domain:** Select this option to clone a WebLogic Domain from an existing reference domain that is already discovered with Cloud Control. It allows you to clone the Middleware Home and its binaries, and the domain configuration.
4. In the Select Source page, depending on your selection, the WebLogic Domain or the Middleware Home to be cloned is displayed.

Figure 15–5 Middleware Provisioning: Source Page

Provisioning

Source Destinations Domain Configuration Schedule Review

Middleware Provisioning : Source

This procedure clones and configures a WebLogic Domain from an existing installation.

Back Step 1 of 5 Next Cancel

Select source from an existing installation

WebLogic Domain EMGC_DOMAIN

The list of WebLogic Domains to select from is automatically filtered and displays only those domains which support the cloning operation.

Host adc2100158.us.oracle.com

Source Information

Component	Location
EMGC_DOMAIN	/net/adc2100158/scratch/bbsubram/view_storage/bbsubram_e120708/work/user_projects/domains/EMGC_DOMA
Middleware Home	/net/adc2100158/scratch/bbsubram/view_storage/bbsubram_e120708/work/middleware
WebLogic Server 10.3	/net/adc2100158/scratch/bbsubram/view_storage/bbsubram_e120708/work/middleware/wlserver_10.3
Oracle Home(s)	
webtierhome	/net/adc2100158/scratch/bbsubram/view_storage/bbsubram_e120708/work/middleware/webtierhome

Host Credentials

Select credential from one of the following options.

Credential Preferred Named New

Preferred Credential Name Normal Host Credentials

Credential Details

Attribute	Value
UserName	bbsubram
Password	*****

More Details

Working Directory /tmp/fmwProvSrc

5. In the Source Information section, the location of the WebLogic Domain, Middleware Home, WebLogic Server or the location of the Middleware Home is displayed.
6. In the Working Directory field, specify the directory on the destination Host on which the cloning related files are temporarily stored. The directory must have sufficient space to store the cloning related files. If this directory is not present, it will be created. When the cloning operation has been completed, the contents of this directory will be deleted.

Note: The Working Directory must not be created under the Middleware Home or the WebLogic Domain Home directory.

7. In the Host Credentials section, enter the host credentials of the machine on which the Administration Server is running. Select one of the following options:
 - **Preferred Credentials:** The preferred credentials stored in the Management Repository are used. The Preferred Credentials option will be available only if it has already been defined in Cloud Control.
 - **Named Credentials:** The credentials of a named profile stored in the Management Repository is used. To use the Named Credentials stored in the Management Repository, you must have already registered each of the preferred credential types with a unique name. Select the desired Named credential from the list available in Credential Name. If you have created all necessary named credentials, you can use them now. If they have not been created, you can create them using this deployment procedure.
 - **New Credentials:** You can override the preferred credentials by specifying a new credential with a unique name and password.
8. Click **Next**. In the Middleware Provisioning: Destinations page, specify the destination hosts on which the Middleware Home or WebLogic Domain is to be cloned.

Figure 15–6 Middleware Provisioning: Destinations Page

9. In the Select Destinations section, click **Add Hosts**. Select a host from the list and specify the operating system credentials for the owner of the Middleware Home on the destination host. The Host Credentials can be Preferred, Named, or New credentials.
10. In the Select Destination Locations section, specify the location of the Middleware Home on the Host machine. You can select one of the following:
 - **Create a New Middleware Home:** Select this option to create a new Middleware Home on the destination host.
 - **Use an Existing Middleware Home:** Select this option to use the existing Middleware Home present on the destination host.
 - **Use a Shared Location:** If you have added more than one host, select this option to use a shared location for all the destination hosts. Specify an absolute path that is accessible by all targets here. If you select this option, the JDK Home Location associated with the Middleware Home and the Oracle Inventory location must also be shared.
11. In the Middleware Home Directory field, enter the full path to the directory in which the Middleware Home is to be created.
12. In the JDK Home Location field, enter the absolute path to the JDK directory to be used on the destination Host. You need to specify this path if a similar configuration is detected on the source machine.
13. In the Working Directory field, specify the directory on the destination Host on which the cloning related files are temporarily stored. This directory must have sufficient space to create the cloning related files. If this directory is not present, it will be created. When the cloning operation has been completed, the directory and its contents will be deleted.

Note:

- The Working Directory must not be created under the Middleware Home or the WebLogic Domain Home directory.
- If the source and destination machines are the same, the Working Directory for the source and destination must be different.

14. Click **Next**. If you selected the Cloning a WebLogic Domain option, the Middleware Provisioning: Domain Configuration page appears. This page contains a set of links to several pages where you can enter the properties that are most likely to be reconfigured like domain name, listen addresses for the administration server and managed servers, Node Manager/Machine configuration, and JDBC data sources. By default, the source domain configuration settings are used as default values for the destination domain. For example, if the source domain has one cluster containing 4 managed servers, the destination domain will also have one cluster with 4 servers but these default values can be changed. For more information on configuring the domain, see *Oracle® Fusion Middleware Creating Domains Using the Configuration Wizard* guide.

Figure 15–7 Domain Configuration: Domain Properties Page

15. In the **Domain Properties** page, enter or modify the following details:

- **Domain Name:** The name of the domain is displayed but can be modified. The generated components for the domain are stored under the specified Domain directory. For example, if you enter mydomain, your domain files are stored (by default) in MW_HOME\user_projects\domains\mydomain. The domain name must not start with a number. The domain name is also listed on the Windows Start menu. For example, if your domain name is mydomain, and the Domain directory is user_projects, you can access commands for the domain by selecting **Oracle WebLogic > user_projects > mydomain** from the Windows Start menu.
- **Domain Administrator Username:** The default Administrator account for the domain. This account is used to boot and connect to the domain's Administration Server. The username must not contain commas, tabs, or any of these characters: < > # | & ? () { }

- **Password:** The password for the Administrator account. The password must be at least eight characters, and must contain at least one numeric character or at least one of the following characters:
 !"#\$%&'()*+,-./:;<=>@[\] ^ _ ` { | } ~
 - **Unique Domain Identifier:** A farm is a collection of components managed by Cloud Control. It can contain an Oracle WebLogic Server domain, one Administration Server, one or more Managed Servers, and the Oracle Middleware components that are installed, configured, and running in the domain. The Unique Domain Identifier is used as a prefix to ensure that the farm names are unique in environments with the same domain name. It is used to name the farm target as a prefix in conjunction with the WebLogic domain name. For example, if the Unique Domain Identifier is farm and the domain name is base_domain then the farm name would be farm_base_domain.
 - **Applications Location:** The directory in which the applications will be deployed on the destination host. By default, this directory is created under the parent directory of the Middleware Home. For example: If the Middleware Home is located at /user/mwh, the application directory is created as /user/applications.
 - **Domain Location:** The location in which your domain directory will be stored. By default, this directory is created under the parent directory of the Middleware Home, but can be changed. For example: If the Middleware Home is located at /user/mwh, the application directory is created as /user/domains. The domain location can be anywhere on the destination host machine or network. On Windows, you must include the drive letter in this path.
16. In the Clusters page, you can modify the name of the cluster, enter the cluster address that identifies the Managed Servers in the cluster, and the messaging mode (multicast or unicast). If you selected Multicast as the Messaging Mode, enter the address and port number that will be dedicated for multicast communications on the cluster.

Note: The destination domain can have the same number of clusters as the source domain. If the source domain has no clusters, you cannot add a cluster in the destination domain.

17. In the Machines page, enter the configuration information for the machines in the domain. A Machine is a logical representation of the system that hosts one or more WebLogic Server instances. The Administration Server and Node Manager use the Machine definition to start remote servers. The machine configurations present in the source domain are listed here. You can modify the configuration details defined for each machine or click **Add Rows** to add one or more machine configurations. Enter the following details:
- **Machine Name:** Enter a valid machine name or modify an existing name. The machine name is used to identify the machine within the WebLogic domain; it does not have to match the network name for the machine. The name must be unique among all component names within the domain.
 - **Node Manager Listen Address:** Enter the listen address used by Node Manager to listen for connection requests. By default, the IP addresses defined

for the local system and localhost are shown in the drop-down list. The default value is the same as specified in the source domain.

Note: If multiple machines are running on the same host, the Node Manager Home location must be different for each host.

- **Node Manager Listen Port:** Enter a valid value for the listen port used by Node Manager to listen for connection requests. The valid Node Manager listen port range is from 1 to 65535. The default value is 5556. The port number must be available on the destination machine.
 - **Node Manager Home:** Enter the directory in which the Node Manager is to be installed. For existing machine configurations, the Node Manager is installed under the parent directory of the Middleware Home directory by default, but this can be modified.
18. In the Servers page, enter the configuration information for the Administration Server and one or Managed servers.

Figure 15–8 Domain Configuration: Domain Properties: Servers Page

The screenshot shows the 'Servers' page in the Oracle Enterprise Manager Provisioning console. The page title is 'Middleware Provisioning : Domain Configuration'. The breadcrumb trail is 'Source Destinations Domain Configuration Schedule Review'. The current step is 'Step 3 of 5'. The page contains two tables for server configuration.

Administration Servers Table:

Name	Host	Listen Address	Listen Port	Enable SSL	SSL Listen Port
EMGC_ADMINSERV	adc2100158.us.oracle.com	adc2100158.us.oracle.com	7001	<input checked="" type="checkbox"/>	7022

Managed Servers Table:

Id	Name	Host	Listen Address	Listen Port	Enable SSL	SSL Listen Port	Max
1	EMGC_OMS1	adc2100158.us.oracle.com	adc2100158.us.oracle.com	7019	<input checked="" type="checkbox"/>	7021	EMG

- **Administration Server:** Enter the following details for the Administration Server:
 - **Name:** Valid names are a string of characters (alphabetic and numeric).
 - **Host:** Select the host on which the Administration Server is to be installed.

Note: The host:port combination for the Administration Server must be unique among all the registered domains. For example, if an Administration Server running on myhost.example.com:7001 has been discovered in Cloud Control, this host name and port number combination cannot be used for a new Administration Server even if the status of the old Administration Server is Down or it has been removed.

- **Listen Address:** Enter the listen address to be used to connect to the Administration Server.
- **Listen Port:** Enter a valid value for the listen port to be used for regular, nonsecure requests (through protocols such as HTTP and T3). The valid

listen port range is from 1 to 65535. The port number you enter here must be available on the destination machine.

- **SSL Listen Port:** If you check the Enable SSL checkbox, enter the number of the SSL Listen Port for secure requests. You must ensure that the port numbers you specify for the Listen Port and SSL Listen Port are available. If you are using the SSL configuration, you must ensure that the security/identity stores are present in the file system under the same path as on the source and are configured with certificates generated for the destination hosts
- **Machine:** Select the machine configuration that is to be associated with the Administration Server.
- **Managed Servers:** You can add or delete the configuration for the Managed Servers. A Managed Server is a WebLogic Server instance to which you deploy Web applications, EJBs, and other resources. Enter the following details:
 - **Name:** Valid server names are a string of characters (alphabetic and numeric). The name must be unique in the domain.
 - **Host:** The host on which the managed server is running.
 - **Listen Address:** Enter the listen address to be used to connect to the Managed Server instance.
 - **Listen Port:** Enter a valid value for the listen port to be used for regular, nonsecure requests (through protocols such as HTTP and T3). The valid listen port range is from 1 to 65535. The port number you enter here must be available on the destination machine.

Note: If a domain was registered on the host with a port number whose status is down, you need to select a different port or manually deregister the domain before launching the deployment procedure.

- **Enable SSL:** Select this check box to enable the SSL listen port. By default, SSL is disabled for all new servers.
 - **SSL Listen Port:** This field is enabled only if you selected the SSL enabled check box. Enter a valid value to be used for secure requests (through protocols such as HTTPS and T3S). The valid listen port range is from 1 to 65535. The port number you enter here must be available on the destination machine.
 - **Machine:** Select the machine configuration that is to be associated with the Managed Server.
 - **Cluster:** Select the cluster that is to be associated with the Managed Server.
19. In the JDBC Data Sources page, enter the configuration information for the data source. A JDBC data source contains a pool of database connections that are created when the data source instance is created—when it is deployed or targeted, or at server startup. Applications look up a data source on the JNDI tree, and then request a connection. When the applications no longer need the connections, they return the connections to the connection pool in the data source.

By default, the cloned domain is configured with the same JDBC data sources as the source domain but it can be changed here. In the Driver field, select the correct

driver from the drop down list. Based on the driver you have selected, enter the URL in the correct format. Select the target from the drop down list and specify the database user name and password.

20. In the Server Startup Mode page, you can optionally start up the Managed Servers and / or the Administration Server.
21. In the JMS page, you can add new JMS persistent stores and JMS servers. A JMS file store is a disk-based file in which persistent messages can be saved. You can modify the JMS file stores configured in your domain. If these are not configured in the source domain, they cannot be configured in the destination domain.
22. In the Security Store and Security Providers pages, you can configure an external database as a data store for various security providers.
23. In the Files page, specify any external files that need to be cloned from the source domain. All the external files must reside in the same directory on the Administration Server host and will be cloned to the same directory on the destination host.
24. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, **Immediately**. If you want to run the procedure later, then select **Later** and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure after the necessary prerequisite checks have been completed** to pause the procedure execution after all prerequisite checks are performed. Click **Next**.
25. On the Review page, review the details you have provided for the Deployment Procedure. If you are satisfied with the details, then click **Submit** to run the Deployment Procedure according to the schedule set. If you want to modify the details, click the **Edit** link in the section to be modified or click **Back** repeatedly to reach the page where you want to make the changes.
26. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the **Status** link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

15.6.2 Cloning a Middleware Home from an Existing Installation

This section covers the procedures involved in cloning a Middleware Home from an existing installation. It covers the following:

- [Prerequisites](#)
- [Deployment Procedure](#)

15.6.2.1 Prerequisites

Before running this deployment procedure, you must meet the following prerequisites:

- The hosts on which the Middleware domains are to be cloned must be discovered targets in Cloud Control.
- The user must have Read permissions on the Middleware Home directory on the host machine on which the Administration Server is running.
- The user must have Write permissions on:

- Working Directory on the host machine which Administration Server is running.
- Working Directory on all destination hosts.
- Middleware directory on all destination hosts.

15.6.2.2 Deployment Procedure

This procedure launches a wizard that enables you to clone an Oracle Middleware Home that is already discovered or registered with Cloud Control. To clone an Oracle Middleware Home, follow these steps:

1. From the **Targets** menu, select **Middleware**.
2. A list of Middleware targets is displayed. Right click on WebLogic Domain target in the list and from the context sensitive menu, select **Provisioning** and then select **Clone Middleware Home**.
3. The Middleware Provisioning: Source page is displayed.

Figure 15–9 Middleware Provisioning: Source Page

The screenshot displays the 'Middleware Provisioning: Source' page. At the top, there is a progress bar with steps: Source, Destinations, Schedule, and Review. Below the progress bar, the page title is 'Middleware Provisioning: Source' and a subtitle reads 'This procedure clones a Middleware Home from an existing installation.' There are 'Back', 'Step 1 of 4', 'Next', and 'Cancel' buttons.

The main content area is titled 'Select source from an existing installation'. It shows the selected 'Middleware Home' path: '/net/adc2100158/scratch/bbsubram/view_storage/bbsubram_e120708/work/middleware'. The host is identified as 'adc2100158.us.oracle.com'.

The 'Source Information' section contains a table with the following data:

Component	Location
Middleware Home	/net/adc2100158/scratch/bbsubram/view_storage/bbsubram_e120708/work/middleware
WebLogic Server 10.3	/net/adc2100158/scratch/bbsubram/view_storage/bbsubram_e120708/work/middleware/wlsrver_10.3
Oracle Home(s)	
webtierhome	/net/adc2100158/scratch/bbsubram/view_storage/bbsubram_e120708/work/middleware/webtierhome

The 'Host Credentials' section prompts the user to 'Select credential from one of the following options.' It includes radio buttons for 'Preferred' (selected), 'Named', and 'New'. Below this, there is a dropdown for 'Preferred Credential Name' set to 'Normal Host Credentials'. A 'Credential Details' table is shown:

Attribute	Value
UserName	bbsubram
Password	*****

At the bottom, there is a 'Working Directory' field with the value '/tmp/fmwProvSrc'.

4. In the Source Information section, the Middleware Home to be cloned is displayed.
5. Follow Steps 6 to 9 as listed in [Section 15.6.1](#).
6. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure to allow me to analyze results after performing prerequisite checks** to pause the procedure execution after all prerequisite checks are performed. Click **Next**.
7. On the Review page, review the details you have provided for the Deployment Procedure. If you are satisfied with the details, then click **Submit** to run the

Deployment Procedure according to the schedule set. If you want to modify the details, click the **Edit** link in the section to be modified or click **Back** repeatedly to reach the page where you want to make the changes.

8. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the **Status** link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to **Debug** and click **Stop** to stop the procedure execution.

15.7 Cloning from a Profile or a Middleware Home Gold Image

This section describes the procedures to clone a WebLogic Domain from a provisioning profile present in the Software Library or a Middleware Home from a Middleware Home Gold Image. It contains the following sections:

- [Cloning from a WebLogic Domain Provisioning Profile](#)
- [Cloning from an Oracle Middleware Home Gold Image](#)

Figure 15–10 and Figure 15–11 show the sequence of operations involved in cloning a WebLogic Domain or Middleware Home from a profile or from a Software Library component.

Figure 15–10 Cloning from a Profile

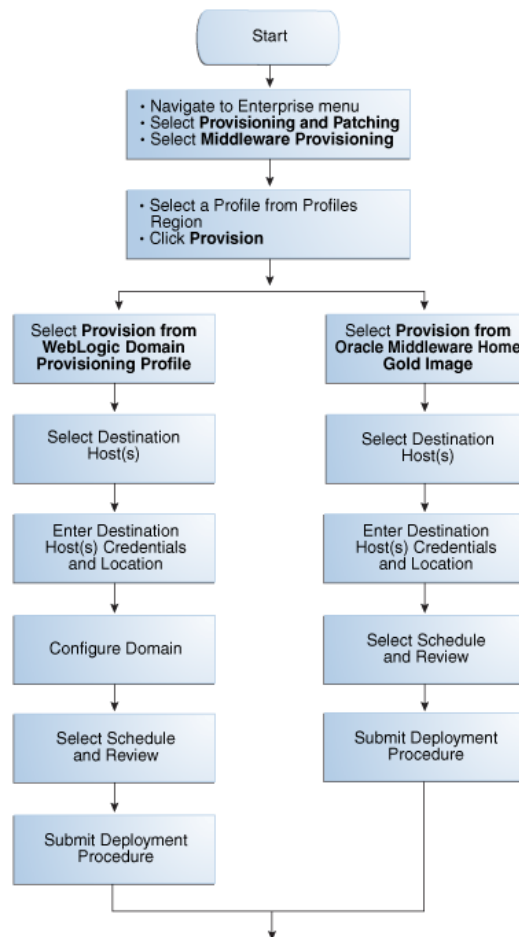
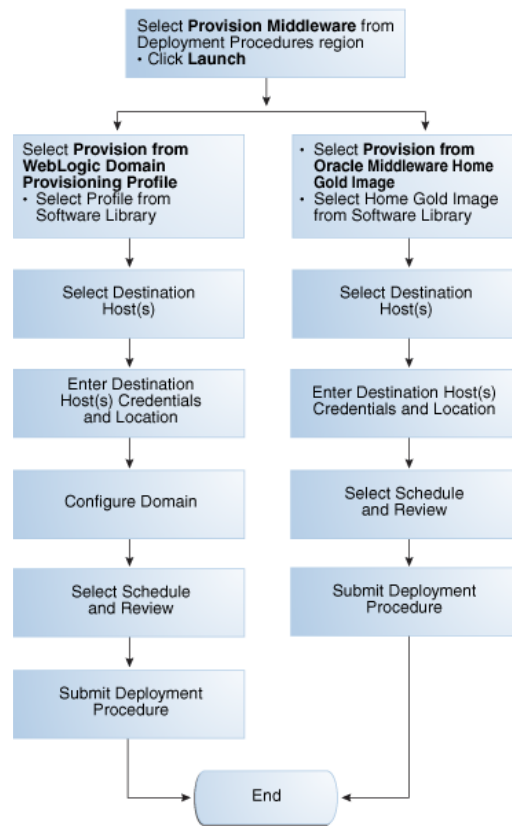


Figure 15–11 Cloning from a Component in the Software Library

15.7.1 Cloning from a WebLogic Domain Provisioning Profile

This section describes the procedures used to clone a WebLogic Domain from a WebLogic Domain Provisioning Profile.

It covers the following:

- [Prerequisites](#)
- [Deployment Procedure](#)

15.7.1.1 Prerequisites

Before running this deployment procedure, you must meet the following prerequisites:

- The user must have Write permissions on:
 - The Working Directory on all destination hosts.
 - Middleware Home on all destination hosts.
- The ports on the Administration Server, Managed Server, and Node Manager must be free.
- A WebLogic Domain Provisioning Profile must be present in the Software Library. For details on creating this profile, see [Section 15.5.1](#).

15.7.1.2 Deployment Procedure

You can clone a WebLogic Domain from a profile present in the Software Library. To clone a WebLogic Domain from a profile, follow these steps:

1. From the Enterprise menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. Select a profile from the Profiles section, and click **Provision**. You can also select the Middleware Provisioning deployment procedure and click **Launch**.
3. In the Source Information section, the selected component and its location is displayed. Click **Next**.
4. In the Middleware Provisioning: Destinations page, specify the destination hosts on which the WebLogic Domain is to be cloned.

Figure 15–12 *Middleware Provisioning: Destination*

Provisioning

Source Destinations Domain Configuration Schedule Review

Middleware Provisioning : Destinations Save Back Step 2 of 5 Next Cancel

Specify the destination hosts on which to clone the source. This deployment procedure requires a Management Agent to be installed and running on each destination host.

Select Destination Hosts

Specify operating system credentials for the owner of the Middleware Home on the destination hosts.

+ Add Hosts ✖ Delete Hosts

ID	* Host
1	SLCO3FJ3.us.oracle.com

Host Credentials

Select credential from one of the following options.

Credential Preferred Named New

Credential Name

Attribute	Value
UserName	aime
Password	*****

[More Details](#)

Select Destination Locations

Specify the way to create destination Middleware Home

Create a new Middleware Home

Use an existing Middleware Home

Use a Shared Location

* Middleware Home Directory

* Working Directory

JDK Home Location

Provide the absolute path of the JDK directory to be used on the destination hosts. This path must be accessible on all destination hosts.

5. Click **Add Hosts** and select a host from the list. Specify the credentials for the destination host. The credentials can be:
 - **Preferred Credentials:** The preferred credentials stored in the Management Repository are used. The Preferred Credentials option will be available only if it has already been defined in Cloud Control.
 - **Named Credentials:** The credentials stored in the Management Repository is used. To use the Named Credentials stored in the Management Repository, you must have already registered each of the preferred credential types with a unique name. Select the desired Named credential from the list available in Credential Name. If you have created all necessary named credentials, you can use them now. If they have not been created, you can create them using this deployment procedure.
 - **New Credentials:** You can override the preferred credentials by specifying a new credential with a unique name and password. These credentials can be different for each host or the same for all the hosts.

6. In the Select Destination Locations section, specify the location of the Middleware Home on the Host machine. The Create a New Middleware Home option is selected by default.
7. In the Middleware Home Directory field, enter the full path to the directory in which the Middleware Home is to be created.
8. In the JDK Home Location field, enter the absolute path to the JDK directory to be used on the destination Host. This field can be edited only if the JDK Home in the source domain is in an external location. If the JDK Home in the source domain is internal and installed in the Middleware Home, this field cannot be edited.

Note: If there are several destination hosts, the location of the Middleware Home, Working Directory, and JDK Home Location is the same across all the hosts.

9. In the Working Directory field, specify the directory on the destination Host on which the cloning related files are temporarily stored. This directory must have sufficient space to store the files. If this directory is not present, it will be created. When the cloning operation has been completed, the directory and its contents will be deleted.
10. Click **Next**. Follow **Steps 13 to 26** as listed in the [Section 15.6.1](#) section.

Note: The **Node Manager Listen Address** must be unique and must be a valid host name or IP address.

15.7.2 Cloning from an Oracle Middleware Home Gold Image

This section describes the procedures used to clone a Middleware Home from an Oracle Middleware Home Gold Image. It covers the following:

- [Prerequisites](#)
- [Deployment Procedure](#)

15.7.2.1 Prerequisites

Before running this deployment procedure, you must meet the following prerequisites:

- The user must have Write permissions on:
 - The Working Directory on all destination hosts.
 - Middleware Home on all destination hosts.
- An Oracle Middleware Home Gold Image must be present in the Software Library. For details on creating this gold image, see [Section 15.5.2](#).

15.7.2.2 Deployment Procedure

You can clone a Middleware Home from a gold image present in the Software Library. This gold image must have been created earlier by pointing to an existing Middleware Home. To clone a Middleware Home from a gold image, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.

- From the Middleware Provisioning Deployment Procedures section, select the Provision Middleware procedure from the list and click **Launch**.
- In the Middleware Provisioning: Source page, select the **Provision from Oracle Middleware Home Gold Image** option. Click the **Search** icon next to the Home Gold Image from Software Library field and select a gold image from the list.

Figure 15–13 Middleware Provisioning (Gold Image): Source

Provisioning

Source Destinations Domain Configuration Schedule Review

Middleware Provisioning : Source Save Back Step 1 of 5 Next Cancel

This procedure clones and configures a Middleware Home and/or WebLogic Domain from the Software Library.

Provision from WebLogic Domain Provisioning Profile
Profile from Software Library

Provision from Oracle Middleware Home Gold Image
Home Gold Image from Software Library win32_soa_patch_FMWHome

Source Information

Component	Location
win32_soa_patch_FMWHome	11DEBNAYAK\win32_soa_patch_FMWHome

- In the Source Information section, the selected component and its location is displayed. Click **Next**.
- In the Middleware Provisioning: Destinations page, specify the destination hosts on which the Middleware Home is to be cloned.

Figure 15–14 Middleware Provisioning (Gold Image): Destination

Provisioning

Source Destinations Domain Configuration Schedule Review

Middleware Provisioning : Destinations Save Back Step 2 of 5 Next Cancel

Specify the destination hosts on which to clone the source. This deployment procedure requires a Management Agent to be installed and running on each destination host.

Select Destination Hosts

Specify operating system credentials for the owner of the Middleware Home on the destination hosts.

+ Add Hosts - Delete Hosts

No	* Host
1	SLC03FJ1.us.oracle.com

Host Credentials

Select credential from one of the following options.

Credential Preferred Named New

Credential Name CS_ALL

Attribute	Value
UserName	aimc
Password	*****

More Details

Select Destination Locations

Specify the way to create destination Middleware Home

Create a new Middleware Home
 Use an existing Middleware Home
 Use a Shared Location

* Middleware Home Directory C:\mwh_soa_patch

* Working Directory C:\Temp\FmwProvDest

JDK Home Location C:\mwh_soa_patch\jrockit_160_24_D1.1-2-4

Provide the absolute path of the JDK directory to be used on the destination hosts. This path must be accessible on all destination hosts.

- Click **Add Hosts** and select a host from the list. Specify the credentials for the destination host. The credentials can be:
 - Preferred Credentials:** The preferred credentials stored in the Management Repository are used. The Preferred Credentials option will be available only if it has already been defined in Cloud Control.

- **Named Credentials:** The credentials of a named profile stored in the Management Repository is used. To use the Named Credentials stored in the Management Repository, you must have already registered each of the preferred credential types with a unique name. Select the desired Named credential from the list available in Credential Name. If you have created all necessary named credentials, you can use them now. If they have not been created, you can create them using this deployment procedure.
 - **New Credentials:** You can override the preferred credentials by specifying a new credential with a unique name and password. These credentials can be different for each host or the same for all the hosts.
7. In the Select Destination Locations section, specify the location of the Middleware Home on the Host machine. The Create a New Middleware Home option is selected by default.
 8. In the Middleware Home Directory field, enter the full path to the directory in which the Middleware Home is to be created.
 9. In the JDK Home Location field, enter the absolute path to the JDK directory to be used on the destination Host. This field can be edited only if the JDK Home in the source domain is in an external location. If the JDK Home in the source domain is internal and installed in the Middleware Home, this field cannot be edited.

Note: If there are several destination hosts, the location of the Middleware Home, Working Directory, and JDK Home Location is the same across all the hosts.

10. In the Working Directory field, specify the directory on the destination Host on which the cloning related files are temporarily stored. This directory must have sufficient space to store the files. If this directory is not present, it will be created. When the cloning operation has been completed, the directory and its contents will be deleted. Click **Next**.
11. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure after the necessary prerequisite checks have been completed** to pause the procedure execution after all prerequisite checks are performed. Click **Next**.
12. On the Review page, review the details you have provided for the Deployment Procedure. If you are satisfied with the details, then click **Submit** to run the Deployment Procedure according to the schedule set. If you want to modify the details, click the **Edit** link in the section to be modified or click **Back** repeatedly to reach the page where you want to make the changes.
13. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the **Status** link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

15.8 Post Deployment Configuration

This section describes the manual configuration steps that need to be performed after cloning or scaling out a WebLogic Domain.

- After the deployment procedure has been successfully completed, you must set the `STARTSCRIPTENABLED=TRUE` in the `nodemanager.properties` file.

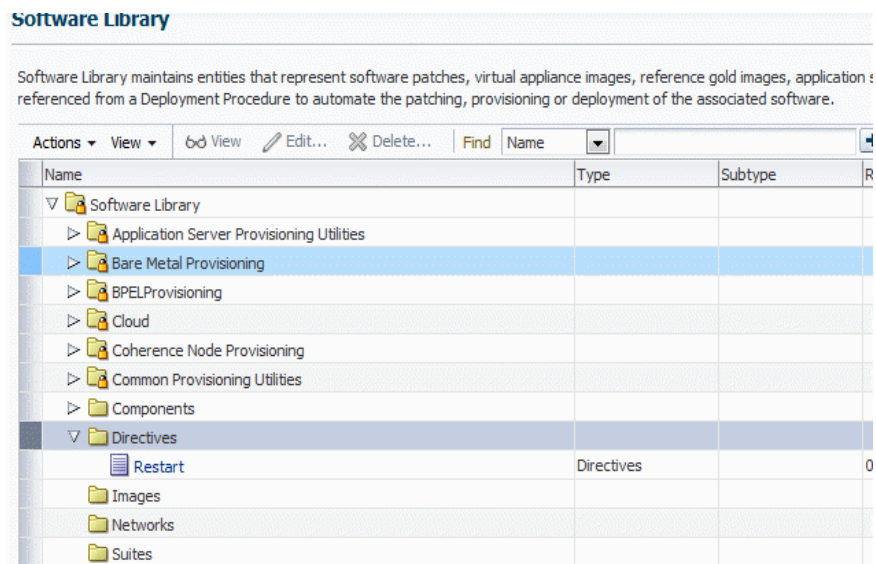
If this property is not set, you may not be able to start the Administration Server from the Console. This is required for WebLogic domains on which additional Oracle Fusion Middleware components (e.g. SOA Suite) have been deployed.

15.9 Customizing the Deployment Procedure

This section describes the procedure to customize the deployment procedure for specific requirements. An example is shown below:

- From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
- Select the Directives folder.

Figure 15–15 Software Library: Directives



- From the **Actions** menu, select **Create Entity**, then select **Directives**.
- In the Create Directives: Describe page, enter a name for the directive step and click **Next**. The Create Directives: Configure page appears.

Figure 15–16 Software Library: Directives: Configure

5. Click **Add** to add one or more command line arguments. Each argument may include a variable to be set later, a prefix and suffix.
6. Select a script type and click **Next** to continue. The Create Directives: Select Files page appears:

Figure 15–17 Create Directives: Select Files

7. Specify a Destination, which is typically a location the Software Library and specify the Source file that is to be uploaded, either from Local Machine or from a remote file system monitored by an Enterprise Manager Agent.
8. Click **Add**. If you are adding from a local machine, in the Add File window, click Browse and select a file less than 25 MB in size, enter a name and click **OK**.

9. If you are adding from a remote location, click **Add**. In the Remote File Browser, specify the login credentials, select the files, click **Add** and **OK** when finished.
10. Click **Save**. You will return to the Software Library page where you can see that a new step has been added.
11. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
12. In the selection list, you can select how the deployment procedure is to be customized. Select **Create Like**, then select the deployment procedure that is to be used and click **Go**.
13. Enter a name for the deployment procedure. Click the **Procedure Variables** tab and click **Add Row** to add one or more procedure variables.
14. Click the **Procedure Steps** tab. You can edit the deployment procedure by selecting an action (such as Enable, Disable, Delete, and so on) to be performed. For example, to insert a custom step, select the step before it is to be inserted, and click **Insert**.

Figure 15–18 Create Directive

15. Specify the general information about the new step. Enter a name for the step and the Insert location.
16. Search for the new step created earlier, select it, and click **Next**. The Create Component Step: Map Properties page appears.

Figure 15–19 Create Component Step: Map Properties

Specify the values for the component and/or directive properties. You can also change the run privilege accordingly.

Directive Run Mode

Run Directive Uncheck this checkbox to skip running the script.

Perform Cleanup Uncheck this checkbox to skip cleaning up the files after step is run.

Component Properties

The selected component has no properties to set.

Directive Properties

oracle_home	<Enter Display Name for var_1>	<Enter Description Here>	Ask User during Procedure Interview
patch_ids	<Enter Display Name for var_2>	<Enter Description Here>	Set Value
stage_dir	<Enter Display Name for var_3>	<Enter Description Here>	Ask User during Procedure Interview
patchsetRelease	<Enter Display Name for var_4>	<Enter Description Here>	Ask User during Procedure Interview
debug_option	<Enter Display Name for var_5>	<Enter Description Here>	Ask User during Procedure Interview
patch_option	<Enter Display Name for var_6>	<Enter Description Here>	Ask User during Procedure Interview
applyBundle	<Enter Display Name for var_7>	<Enter Description Here>	Ask User during Procedure Interview

Credentials

Credential Usage: Normal
Credential Usage in the Target List to be applied for this Step.

17. You can decide the way you want to map the argument in your script. You can select:
- Set Value (set value for the variable now)
 - Choose Variable (bind it to existing data in the deployment procedure)
 - Ask User during Procedure Interview (user enters value when the deployment procedure is launched)

For example, you can choose to set the value for `var_1` at run-time and value of `var_2` now, you can specify the directive properties as required.

18. Click **Next**. Review the information and click **Finish**. You will return to the Procedure Steps page where you can see the deployment procedure has now been added. Click **Save and Close** to return to the Procedure Library page.
19. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
20. Select the newly created deployment procedure and click **Launch**.
21. Follow the same steps as the Middleware Provisioning. If a custom variable needs to be set at run time, specify the appropriate value and click **Next**.
22. Submit the deployment procedure with the newly created step.

15.10 Creating an Oracle Virtual Server Component

Follow these steps to create an operating system component:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. From the Software Library Home, from the **Actions** menu, select **Create Folder**.
3. In the Create Folder popup, specify a **Name** and **Description** for the folder and select the folder location.
4. From the **Actions** menu, select **Create Entity** and then **Bare Metal Provisioning Components**.

5. In the Create Entity: Bare Metal Provisioning Components dialog box, select **Oracle Virtual Server Component** and click **Continue**.
6. On the Describe page, enter the **Name**, **Description**, and **Other Attributes** that describe the entity.

Note: The component name must be unique to the parent folder that it resides in. Sometime even when you enter a unique name, it may report a conflict, this is because there could be an entity with the same name in the folder that is not visible to you, as you do not have view privilege on it.

Click **+Add** to attach files that describe the entity better like readme, collateral, licensing, and so on. Ensure that the file size is less than 2 MB.

In the **Notes** field, include information related to the entity like changes being made to the entity or modification history that you want to track.
7. In the Basic Operating System page, select a **Time Zone** and specify the **Root Password** and the **OVM Agent Password**.

In the Operating System Users List, add the users for the operating system by specifying the **User Name**, **Password**, **Primary Group**, and **Additional Groups**. Specify if you want to **Enable Sudo Access** for the user.

Click **Next**.
8. In the Advanced Configuration page, specify the Dom0 Configuration, Boot Configurations, and Additional OS Details as explained in the tables.

Click **Next**.
9. In the Review page, verify the information and click **Finish**.

The oracle virtual server component will be saved in the Software Library with the status Ready.

Table 15–2 Dom0 Configuration

Element	Description
Dom0 Memory	
Advanced Configuration and Power Interface	

Table 15–3 Additional OS Details

Element	Description
Mount Point Settings	Specify entries for the /etc/fstab file. You can specify mount points on the newly provisioned Linux machine. By default, mount point settings from the reference Linux machine are inherited.
NIS Settings	Specify entries for the /etc/yp.conf file. You can specify NIS settings for the newly provisioned Linux machine. By default, NIS settings from the reference Linux machine are inherited.
NTP Settings	Specify entries for the /etc/ntp.conf file. You can specify NTP settings for the newly provisioned Linux machine. By default, NTP settings from the reference Linux machine are inherited.
Kernel Parameter Settings	Specify scripts for Kernel Parameters.

Table 15–3 (Cont.) Additional OS Details

Element	Description
Initab Settings	Specify settings for /etc/inittab file. All processes are started as part of init operation in boot process. Init operation decides the processes that will start on booting of a machine or when runlevel changes.
Firewall Settings	Specify firewall settings for the Linux target. Firewall settings are disabled by default and can be configured. Make sure that the port used by Management Agent is open for its communication with the Management Service. By default, Management Agent uses port 3872 or a port number in the range 1830-1849, unless configured to use some other port.

Table 15–4 Boot Configuration and Configuration Scripts

Element	Description
Post Install Script	Specify any set of commands that need to be executed on the newly provisioned machine. These commands will be appended to the post section of the kickstart file.
First Boot Script	Specify any set of commands that need to be executed on the newly provisioned machine when it starts up for the first time.

Scaling Up / Scaling Out WebLogic Domains

This chapter explains how you can scale up and scale out a WebLogic Domain using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [About Scaling Up / Scaling Out WebLogic Domains](#)
- [Prerequisites for Designers and Operators](#)
- [Prerequisites for the Deployment Procedure](#)
- [Running the Scale Up / Scale Out Middleware Deployment Procedure](#)
- [Middleware Provisioning and Scale Up / Scale Out Best Practices](#)

16.1 About Scaling Up / Scaling Out WebLogic Domains

A WebLogic Domain consists of a set of managed servers running independently or in a cluster, sharing the distributed resources. A WebLogic Server cluster consists of multiple WebLogic managed servers running simultaneously and working together to provide increased scalability and reliability. The server instances that constitute a cluster can run on the same machine, or be located on different machines. You can increase a cluster's capacity by adding additional server instances to the cluster on an existing machine, or by adding machines to the cluster to host the new server instances. You can use the Domain Scale Up / Scale Out deployment procedure to automate the scaling up or scaling out of a domain. You can:

- Scale up a domain by adding or cloning a managed server to a host that already exists in the domain or cluster.
- Scale out a domain by adding or cloning a managed server to a host that is not present in the domain or cluster.

16.2 Prerequisites for Designers and Operators

This section describes the prerequisites required by Designer and Operator users before the Middleware Provisioning deployment procedures can be executed. It contains the following sections:

- [Prerequisites for Designers](#)
- [Prerequisites for Operators](#)
- [Additional Prerequisites on Windows](#)

16.2.1 Prerequisites for Designers

Designers are lead administrators with increased privileges on Deployment Procedures and Software Library. For more details, see *Overview of User Accounts*.

Following are the prerequisites required for designers to create components in the library, customize the deployment procedure, and create and save deployment procedures for future usage by operators.

- Ensure that you meet the infrastructure requirements described in [Chapter 2](#).
- Discover and monitor the destination hosts in Cloud Control. For this purpose, you need the latest version of Oracle Management Agent (Management Agent) on the destination hosts. For more information refer to the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*. Ensure that the agents are installed in the same location on all hosts.
- Set up the Oracle Software Library (Software Library). Ensure that the required components are available in the Software Library. For information about creating them, see [Section 2.2](#).
- Store the operating system credentials of the destination hosts as preferred credentials in Oracle Management Repository (Management Repository) or use Named Credentials.

If you are using SUDO, PowerBroker, see [Section 2.3.3](#) for information on setting up these authentication utilities.

- You must have **Write** permissions on the following locations:
 - Oracle base directory for Grid Infrastructure where diagnostic data files related to Grid Infrastructure can be stored.
 - Grid Infrastructure software directory where Grid Infrastructure software can be provisioned.
- You must have **Operator** target privileges on the destination host machines.
- The domain being scaled up / out should not be in Edit mode. One more prerequisite, domain must not be in edit mode already before scheduling a scale up/out DP. Otherwise an corresponding error message would be pop out.

16.2.2 Prerequisites for Operators

Operators are administrators who have restricted privileges on a Deployment Procedure and Software Library. Normally, operators can view and submit a deployment procedure. The Designer user may also grant the Operator the necessary privileges on any targets or entities. For more details, see *Overview of User Accounts*.

Following are the prerequisites for operators who will run the deployment procedures:

- You must have permissions to view credentials (set and locked by the designer), view targets, submit jobs, and launch deployment procedures.
- You must have **Operator** target privileges on the destination host machines.
- The Administration Server must use a non-SSL port for the scale up / scale out operations.

16.2.3 Additional Prerequisites on Windows

Following are the additional prerequisites required when you run the deployment procedures on Windows:

- The Operating System user must be part of the Administrators Group.
- Ensure that directory paths and locations you specify are in the Windows standard format.

16.3 Prerequisites for the Deployment Procedure

Before running the Scale Up / Scale Out Middleware deployment procedure, meet the following prerequisites:

- The WebLogic Domain that is scaled up / scaled out must be an existing domain that has been discovered with Cloud Control.
- If you are scaling out a domain, ensure that the destination machine contains sufficient space. If the size of the Middleware Home on the source machine is 3 GB, you need approximately 3 GB in the working directory on the source and destination machines. Additionally, the destination machine should also have 3 GB of space for the Middleware Home. The working directory is cleaned up after deployment procedure has been successfully completed.
- The Middleware Home directory you specify on the destination machine must be a new directory or must be empty.
- The Management Agent must be installed on the source (where the Administration Server is running) and the destination machines. The Administration Server for the domain must be up and running.
- The Administration Server and Managed Server (being cloned) must be up and running before you run the deployment procedure.
- The Managed Server and Node Manager ports must be free.
- For scaling out a domain, the user must have the following permissions:
 - Read permissions on:
 - Administration Server Host Middleware Directory
 - Administration Server Host Domain Directory
 - Write permissions on:
 - Administration Server Host Working Directory
 - Working Directory of all the destination Managed Server hosts
 - Middleware Directory of all the destination Managed Server hosts
 - Domain Directory of all the destination Managed Server hosts
- For scaling up a domain, the user must have the following permissions:
 - Read permissions on:
 - Administration Server Host Working Directory
 - Domain Directory of all the destination Managed Server hosts
- The domain being scaled up / out should not be in Edit mode. Ensure that there is a running WebLogic Console for this domain.

- If you choose to associate the Node Manager with an existing machine, you must ensure that the Node Manager is up and running. If the Node Manager is down or unreachable, the deployment procedure will fail.

16.4 Running the Scale Up / Scale Out Middleware Deployment Procedure

To scale up / scale out a WebLogic Domain, follow these steps:

1. From the **Targets** menu, select **Middleware**.
2. A list of Middleware targets is displayed. Find the WebLogic Domain that you want to use as the source for the cloning operation. Right click on that WebLogic Domain to access the context sensitive menu. From the menu, select **Provisioning** and **Scale Up / Scale Out WebLogic Domain**. The WebLogic Domain Scale Up: Source page is displayed.
3. In the Source Information section, the details of the source domain including the Middleware Home, WebLogic Server Home, and the Middleware Domain Location are displayed.
4. Enter the credentials for the Administration Server Console and Host Credentials. For more information on registering a name for the preferred credentials, see Managing Named Credentials.
 - Preferred Credentials: The preferred credentials stored in the Management Repository are used. The Preferred Credentials option will be available only if it has already been defined in Cloud Control.
 - Named Credentials: The credentials stored in the Management Repository is used. To use the Named Credentials stored in the Management Repository, you must have already registered each of the preferred credential types with a unique name. Select the desired Named credential from the list available in Credential Name. If you have created all necessary named credentials, you can use them now. If they have not been created, you can create them using this deployment procedure.
 - New Credentials: You can override the preferred credentials by specifying a new credential with a unique name and password.
5. In the Working Directory field, specify the directory on the Administration Server machine on which the domain scale up related files are temporarily stored. If this directory is not present, it will be created. When the scale up operation has been completed, the directory and its contents will be deleted.

Note: The Working Directory must not be created under the Middleware Home or the WebLogic Domain Home directory.

6. Click **Next**. The WebLogic Domain Scale Up: Managed Servers page is displayed.
7. Select a domain or a cluster from the left panel. You can then do the following:
 - Click **Add Server** in the left panel. A new server appears in the tree in the left panel. Click on the newly added server and enter the configuration details on the right panel. In the Managed Server section, enter the name of the host on which the managed server is to be added, the name of the new server, listen address, port, and the SSL port if applicable. If you checked the Enable SSL checkbox, enter the number of the SSL port for secure requests. The port

numbers you specify for the Listen Port and the SSL Listen Port must be available on the target machine.

- **Host Credentials:** Enter the credentials for the Managed Server host. You can choose Preferred Credentials, Named Credentials, or New Credentials. Ensure that the same credentials are used for multiple destination hosts.
 - **Software Installation:** The location of the domain and the Middleware Home on the new Managed Server are displayed. These locations will be the same as those present on the Administration Server. In the Working Directory field, specify the path to the temporary directory that will be created on each Managed Server host. This directory is used to store provisioning scripts and will be cleaned up when the deployment procedure has been successfully completed.
 - Select a server from the list and click **Add Server and Copy Attributes** in the left panel. A new server which is a copy of the one you selected will be created. You must configure the new server to proceed with the provisioning.
 - Select a server that you have created from the list and click the **Delete Server**. The selected Managed Server will not be created as part of this scale up/out operation.
8. In the Configure Machines section, you can choose to:
- **Do not associate with any machine (Node Manager):** If you select this option, the Node Manager is not associated with the machine and you cannot use the Node Manager console to start the Managed Server Host.
 - **Create a new machine (Node Manager):** Select this option to create a new machine and specify the machine name, node manager address, and port number. If the Node Manager is not up and running, check to ensure that there is no address or port conflict.
 - **Associate with an existing machine (Node Manager):** Select this option to associate the Node Manager with an existing machine. You must select the machine with which the Node Manager is to be associated from the Machine Name drop down list.

Note: To perform administrative operations such as start and stop from the Enterprise Manager Cloud Control, the Node Manager must be configured and running on the machine.

9. In the Software Installation section, in the Working Directory field, enter the full path to the directory on which the files required for scale up will be staged.
10. In the Managed Server Credentials section, enter the user name and password for the host on which the managed server is to be created.
11. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure after the necessary prerequisite checks have been completed** to pause the procedure execution after all prerequisite checks are performed. Click **Next**.

12. On the Review page, review the details you have provided for the Deployment Procedure. If you are satisfied with the details, then click **Submit** to run the Deployment Procedure according to the schedule set. If you want to modify the details, click the **Edit** link in the section to be modified or click **Back** repeatedly to reach the page where you want to make the changes.
13. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the **Status** link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

16.5 Middleware Provisioning and Scale Up / Scale Out Best Practices

This section lists some of the best practices to be followed while using the Middleware Provisioning deployment procedure.

- **Configuration of the source domain should not be changed:** While executing these deployment procedures, ensure that no administrative activities (such as configuration changes on the source domain and software patching) are actively performed on the source domain. If you change the configuration, the managed server may not respond to requests and the Administration Server will have an Unknown status.
- **Provisioning on the same machine:** If you are using the Deployment Procedure to provision or scale up to the same machine as the source, the working directory on the source and target machines is populated by default. If these values are changed, you must ensure that the working directory on the source and the destination machines are different. For example, if the working directory is `/tmp/source` for the source machine, it could be `/tmp/dest` on the destination directory. You must also ensure that the listen port number and SSL port numbers (if enabled) for the Administration Server and Managed Server are different on the source and destination servers.
- **Unique Farm Prefix:** While using the Provision Middleware Deployment Procedure, ensure that the farm prefix is unique. The farm prefix gets appended to the domain name to uniquely identify a given domain in Cloud Control.
- **JDBC Configuration:** While configuring the JDBC data sources, the database user and schema owner must enter appropriate passwords.
- **Custom Java Applications and their Deployment Plan:** These deployment procedures support custom java applications in staged mode. Externally staged applications need to be manually deployed. For instructions on manual deployment, see the *WebLogic Administration Guide*.
- **Multi NIC Machines:** If the destination machine is a multi NIC system, enter a listen address that is accessible to both the Administration Server and Managed Server.

Deploying / Redeploying / Undeploying Java EE Applications

This chapter explains how you can deploy, undeploy, and redeploy Java EE Applications using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Deploying, Undeploying, or Redeploying Java EE Applications](#)
- [Getting Started](#)
- [Prerequisites](#)
- [Creating a Java EE Application Component](#)
- [Java EE Applications Deployment Procedure](#)

17.1 Deploying, Undeploying, or Redeploying Java EE Applications

This deployment procedure supports deployment of Java EE Applications packaged into `.ear`, `.war`, `.jar` or `.rar` files as per Java EE specifications. Administrators can now use Cloud Control to deploy, redeploy, and undeploy one or more Java EE applications and need not drill down into the WebLogic Server or the Fusion Middleware Administration Console to perform these tasks. The Java EE applications need to be pre-configured before you add them to the Cloud Control Software Library. You can deploy a pre-configured Java EE application to one or more WebLogic domains in Cloud Control.

The Java EE Application Provisioning Wizard offers GUI-rich interactive screens that allow you to deploy / redeploy to, or undeploy a pre-configured Java EE application from one or more WebLogic Domains.

17.2 Getting Started

This section provides an overview of the steps involved in deploying, redeploying, and undeploying Java EE Applications. The Deploy / Undeploy Java EE Applications Deployment Procedure allows you perform the following operations:

- Deploy
- Undeploy
- Redeploy

Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision a Java EE Application. Click the

reference links provided against the steps to reach the relevant sections that provide more information.

Table 17–1 Getting Started with Deploying, Undeploying, or Redeploying a Java EE Application

Step	Description	Reference Links
Step 1	<p>Understanding the Deployment Procedure</p> <p>Understand the Deployment Procedures offered by Cloud Control to deploy, undeploy, or redeploy a Java EE Application. Know how the Deployment Procedures function, what use cases it covers, and so on.</p>	To learn about the Deployment Procedure, see Section 17.1 .
Step 2	<p>Selecting the Use Case</p> <p>This chapter covers the use cases for deploying, undeploying, and redeploying Java EE Application. Select the use case that best matches your requirement.</p>	<ul style="list-style-type: none"> ■ To deploy a Java EE Application, see Section 17.5.1 ■ To redeploy a Java EE Application, see Section 17.5.2 ■ To undeploy a Java EE Application, see Section 17.5.3
Step 3	<p>Meeting the Prerequisites</p> <p>Before you run the Deployment Procedure, you must meet the prerequisites, such as configuring the Software Library and creating components to be provisioned as part of the Deploy / Undeploy Java EE Application deployment procedure.</p>	To learn about the prerequisites for deploying, undeploying or redeploying Java EE Application, see Section 17.3 .
Step 4	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully deploy, redeploy, or undeploy one or more Java EE applications.</p>	To run the Deploy / Undeploy Java EE Applications Deployment Procedure, follow the steps explained in Section 17.5 .

17.3 Prerequisites

Before running the Deploy / Undeploy Java EE Applications Deployment Procedure, ensure that the following prerequisites are met:

- The Management Agent must be installed on the hosts on which the Java EE Application is to be deployed, redeployed, or undeployed.
- The destination machine must contain sufficient space.
- The plug-ins required for this deployment procedure must be deployed to the Management Agent on the destination machines.
- Ensure that the Software Library is configured. The archives and other related files must be present in the Software Library. **<Aravind: please add a link to the Software Library chapter>**
- Preferred credentials must be set on all OMS hosts.

17.4 Creating a Java EE Application Component

You can create a Java EE Application component which contains the archive, deployment plan, predeploy, postdeploy, target execution scripts, and other files required for deploying the Java EE application. To create a Java EE Application component, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. Create a folder or select a folder from the Software Library, select **Create Entity**, then select **Component**.
3. From the Create Entity: Component window, select Java EE Application and click **Continue**.
4. In the Create Java EE Application: Describe page, enter the Name, Description, and click **Next**.
5. In the Create Entity: Select Files page, select one or more files to be associated with the Java EE Application. You can upload files from a storage location in the Software Library. For Software Library to become usable, at least one upload file location must be configured. In the Specify Destination section, click the **Browse** button in the Upload Location field. Select either of the following:

- **OMS Shared File System:** An OMS Shared File System location is required to be shared (or mounted) across all the Oracle Management Server (OMS) hosts. This option is ideal for UNIX systems.

For single OMS environments, you can configure the Software Library either on the host where the OMS is running or in a shared location, so that it is accessible to all the OMS hosts. For multiple OMS environments, Oracle recommends that you configure the Software Library in a shared location so that the storage is accessible through NFS mount points to all Oracle Management Servers in the environment.

- **OMS Agent File System:** An OMS Agent File System location is a location that is accessible to one of the OMS host's Agent. This option is ideal for OMS installed on Windows hosts. By selecting this option for uploading files, you can avoid sharing a location between all participating OMS hosts.

Credentials must be set before using an OMS Shared File System or OMS Agent File System. For an OMS Shared File System, normal host credentials must be set before configuring a storage location. However, for OMS Agent File System location configuration, a credential (preferred or named) has to be specified.

6. In the Specify Source section, you can add the standard Java EE archive files such as `.ear`, `.war`, `.jar`, `.rar` and other optional files such pre and post-deploy scripts, target execution script, execution plan and additional files. You can either upload each file separately (Individual Files) or upload a zip file (Zip File) that contains the `JavaEEAppComp.manifest` file. You can upload the files from:
 - **Local Filesystem:** Click **Browse** and upload the files from your local system.
 - **Agent Filesystem:** You can upload the files from a remote filesystem monitored by the Management Agent. Click **Browse** and select a host machine from the list and click **Select**. Click **Add**. The Remote File Browser window is displayed. Click the **Login As** button and enter the credentials for the host machine. Specify the location in which the files are present, select one or more

archive related files and click **Add**. The selected files are listed in the Current Selection section. Click **OK** to return to the Create Entity: Select Files page.

7. The files are listed in the table. Specify the type of the file by selecting the options in the Type field. Click **Next**.
8. Review and verify the information entered so far. Click **Save and Upload** to upload the files and create the Java EE Application component.

17.5 Java EE Applications Deployment Procedure

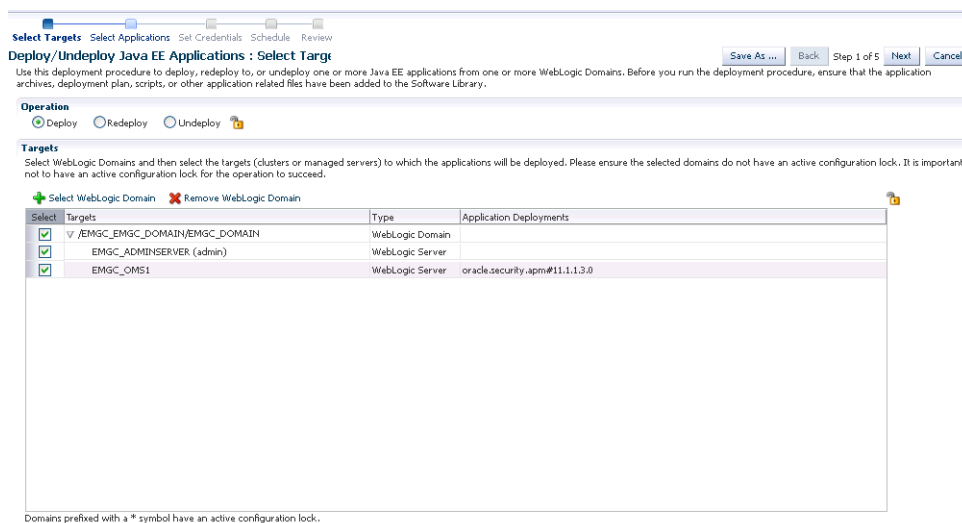
This section describes the Java EE Application deployment procedure. It covers the following:

- Deploying a Java EE Application
- Undeploying a Java EE Application
- Redeploying a Java EE Application

17.5.1 Deploying a Java EE Application

Follow these steps to deploy a Java EE Application:

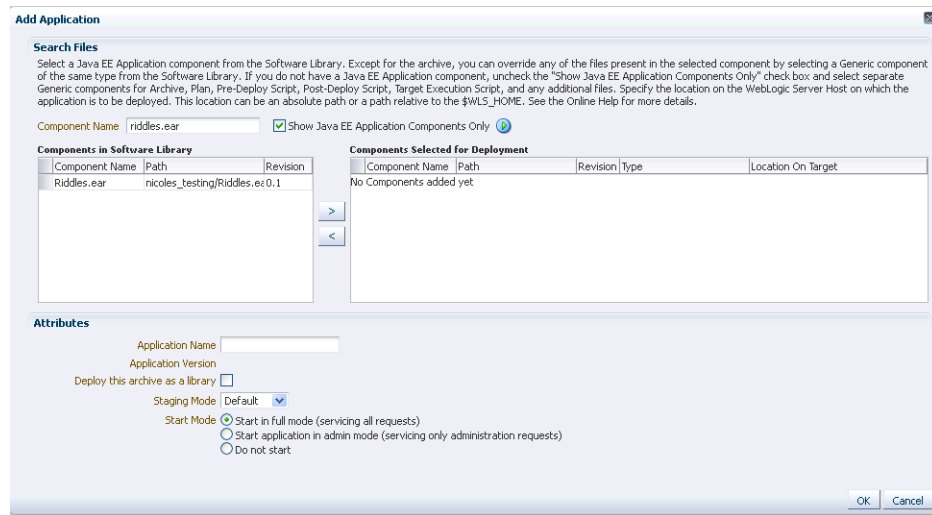
1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. Select the Java EE Application procedure from the list and click **Launch**. You can also use the following method to launch the deployment procedure:
 - Click **Middleware** from the Targets menu.
 - Right click on a WebLogic Domain from the list and from the context sensitive menu, select **Provisioning**, then select **Deploy / Undeploy Java EE Applications**.
 - In the Deployment Procedure Manager page, select the Java EE Application Provisioning procedure and click **Launch**.
3. In the Deploy/Undeploy Java EE Applications: Select Targets page, choose the **Deploy** operation.

Figure 17–1 Deploy / Undeploy Java EE Applications: Select Target

4. Select WebLogic Domains and select the targets on which the Java EE application is to be deployed. Click **Add WebLogic Domains**. Choose one or more WebLogic domains from the list and click **Select**.

Note: You can customize the deployment procedure by locking certain features. You can lock an operation, a target, or an application. Before you proceed with the deployment, you must ensure that the selected domains do not have an active configuration lock. If the selected domains are locked, click the **Lock** icon to unlock the configuration lock.

5. The selected WebLogic domains are listed in the Targets table. Select the targets (clusters or managed servers) for each domain and click **Next**.
6. In the Deploy / Undeploy Java EE Applications: Select Applications page, add the archives and other related files that are to be deployed from the Software Library. Click **Add** to select one or more archives and other application related files or components from the Software Library. The Add Application popup is displayed. In the Component Name field, enter a file name or a wild card pattern to search for and retrieve components from the Software Library. Select the **Show Java EE Application Components Only** checkbox to list only the Java EE Application components in the Components in Software Library column. Select the archives and click the right arrow to move them to the Components Selected for Deployment section.

Figure 17–2 Deploy / Undeploy Java EE Applications: Add Applications

7. In the Type field, the type of each component is displayed. The Type can be:
 - Archive: This is the archive file which can be a .ear, .war, .jar, or .rar file.
 - Plan: This is an .xml file containing the deployment options for this application.
 - Pre Deploy Script: This is a script containing WLST commands. The Management Agent runs this script on the Administration Server of each WebLogic domain before the application is deployed. You can use this script to create data sources, JMS end points, and any other resources that might be needed by the application that is being deployed.
 - Post Deploy Script: This is a WLST script that is executed by the Management Agent on the Administration Server after the application is deployed. You can use this script to perform any post deployment configuration. For example, if you need to roll back and undo the changes made by the pre deploy script, you can select this option.

Note: The archive, plan, predeploy, and postdeploy scripts can be moved only to the Administration Server.

- Additional File: You can add one or more files that will be required by the application that are not part of the application archive. These files can be of any type and can be moved only to the selected targets (managed servers and clusters).
 - Target Execution Script: These scripts can be used to set up the required environment or replace tokens in the additional files like property files. These scripts will be executed on selected targets.
8. In the Location On Target field, for each component, specify the location on the WebLogic Server Host on which the application is to be deployed. This can be an absolute path or relative to the \$WLS_HOME for the selected targets.
 9. After selecting the required files for deployment, enter a unique name for the application and specify the Staging Mode which can be:

- Default: Each server in the WebLogic Domain maintains two attributes which are Staging Mode and StagingDirectoryName. The Staging Mode is the default staging mode for the server and StagingDirectoryName is the location on which the staged files are stored. Select this option to use the default staging mode for all the targets.
 - Stage: Select this option if the archive files should be moved to the destination machine.
 - No Stage: Select this option if the archive files should not be moved to the destination machine.
10. Select the Deploy this archive as library option if the application needs to be deployed as a shared library. You can select this option if one or more applications need the same set of files.
 11. Select the Start Mode for deployment which can be:
 - Start in full mode (servicing all requests): Select this option to make the deployed application available to all users.
 - Start application in admin mode (servicing only administration requests): If you select this option, the deployed application is available only to the Administrator.
 - Do not start: The application is deployed but not started. You can select this option if any manual post-deployment configuration is required.
 12. Click **OK** to add the archive and return to the Select Applications page. You can add more archives or click **Next** to proceed. If you have added more than one archive, select the **Skip on Failure** checkbox to skip any failed deployments and continue deploying the remaining applications.
 13. Click the **Lock** icon to lock the fields you have configured.

Note: The Designer can lock the fields after configuring them. This ensures that the Operator can run the deployment procedure with minimal input.

14. Click **Next**. Specify the credentials for each domain you have selected, the host on which the Administration Server is running, and the hosts to which the additional files or execution scripts are to be moved. You can choose:
 - Preferred Credentials: This option is selected by default and the preferred credentials stored in the Management Repository are used. This option is available only if it has already been defined in Cloud Control.
 - Named Credentials: A named credential specifies the authentication information for a user and can be a combination of username / password, public and private key pair, and can be used to perform provisioning, patching, run jobs, and other system management tasks.
 - New Credentials: You can override the preferred credentials and specify a separate set of credentials for each host and WebLogic domain being deployed.

For more information on setting up the credentials, see the *Enterprise Manager Security* chapter in the *Enterprise Manager Administration Guide*.

15. Click the **Lock** icon to lock the fields you have configured. These fields cannot be edited once they are locked.

16. In the Schedule Deployment page, you can schedule the date on which the Java EE Application deployment procedure should be executed.
17. Click **Next**. On the Review page, review the details you have provided for the Deployment Procedure. If you are satisfied with the details, then click **Submit** to run the Deployment Procedure according to the schedule set. If you want to modify the details, click the Edit link in the section to be modified or click **Back** repeatedly to reach the page where you want to make the changes.

After you submit the deployment procedure, you will return to the Procedure Activity page where you can view the status of the Deployment Procedure. After the Java EE Application has been deployed, you can search for the target and navigate to the Target Home page.

17.5.2 Redeploying a Java EE Application

Follow these steps to redeploy a Java EE application:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. Select the Java EE Application procedure from the list and click **Launch**. You can also use the following method to launch the deployment procedure:
 - Click **Middleware** from the Targets menu.
 - Right click on a WebLogic Domain from the list and from the context sensitive menu, select **Provisioning**, then select Deploy / Undeploy Java EE Applications.
 - In the Deployment Procedure Manager page, select the Java EE Application Provisioning procedure and click **Launch**.
3. In the Select Targets page, choose the Redeploy operation.

Note: Click the **Lock** icon to lock an operation or the fields you are configuring in any of the pages in the wizard. Once the fields have been locked, the Operator needs to provide minimal input while running the deployment procedure.

4. Click Add WebLogic Domains to add one or more WebLogic domains. In the list of targets displayed, choose a target and click Select.
5. The deployment targets are listed in the Targets table. Select the applications that need to be redeployed and click Next.
6. In the Select Applications page, a list of applications that can be redeployed are displayed. Select an application and click Edit to modify the archive details and other application related files. In the Application Details window, enter a file name or a wild card pattern to search for and retrieve files from the Software Library. Select the archives and click the right arrow to move them to the Components Selected for Deployment section.
7. In the Type field, the type of each component is displayed. The Type can be:
 - Archive: This is the archive file which can be a .ear, .war, .jar, or .rar file.
 - Plan: This is an .xml file containing the deployment options for this application.

- Pre Deploy Script: This is a script containing WLST commands. The Management Agent runs this script on the Administration Server of each WebLogic domain before the application is deployed. You can use this script to create data sources, JMS end points, and any other resources that might be needed by the application that is being deployed.
- Post Deploy Script: This is a WLST script that is executed by Management Agent on the Administration Server after the application is deployed. You can use this script to perform any post deployment configuration. For example, if you need to roll back and undo the changes made by the pre deploy script, you can select this option.

Note: The archive, plan, predeploy, and postdeploy scripts can be moved only to the Administration Server.

- Additional File: You can add one or more files that will be required by the application that are not part of the application archive. These files can be of any type and can be moved only to the selected targets (managed servers and clusters).
 - Target Execution Script: These scripts can be used to set up the required environment or replace tokens in the additional files like property files. These scripts will be executed on selected targets.
8. Review the default location on the target machine on which the component will reside. This can be an absolute path or relative to the \$WLS_HOME for the selected targets.
 9. After selecting the required files for deployment, enter a unique name for the application and specify the Staging Mode which can be:
 - Default: Each server in the WebLogic Domain maintains two attributes which are Staging Mode and StagingDirectoryName. The Staging Mode is the default staging mode for the server and StagingDirectoryName is the location on which the staged files are stored. Select this option to use the default staging mode for all the targets.
 - Stage: Select this option if the archive files should be moved to the destination machine.
 - No Stage: Select this option if the archive files should not be moved to the destination machine.
 10. Select the Start Mode for deployment which can be:
 - Start in full mode (servicing all requests): Select this option to make the deployed application available to all users.
 - Start application in admin mode (servicing only administration requests): If you select this option, the deployed application is available only to the Administrator.
 - Do not start: The application is deployed but not started. You can select this option if any post-deployment configuration is required.
 11. Specify the Retirement Policy for the application. You can select:
 - Allow the application to finish its current sessions and then retire: Select this option if all the current sessions should be completed before retirement.

- Retire the previous version after retire timeout: Specify a timeout period after which the application will be automatically retired.
12. Click **OK** to add the archive and return to the Select Applications page. You can add more archives or click **Next** to proceed. If you have added more than one archive, select the **Skip on Failure** checkbox to skip any failed deployments and continue deploying the remaining applications.
 13. Click the **Lock** icon to lock the fields you have configured. These fields cannot be edited once they are locked.
 14. Click **Next**. Specify the credentials for each domain you have selected, the host on which the Administration Server is running, and the hosts to which the additional files or execution scripts are to be moved. You can choose:
 - Preferred Credentials: This option is selected by default and the preferred credentials stored in the Management Repository are used. This option is available only if it has already been defined in Cloud Control.
 - Named Credentials: A named credential specifies the authentication information for a user and can be a combination of username / password, public and private key pair, and can be used to perform provisioning, patching, run jobs, and other system management tasks.
 - New Credentials: You can override the preferred credentials and specify a separate set of credentials for each host and WebLogic domain being deployed.

For more information on setting up the credentials, see the *Enterprise Manager Security* chapter in the *Enterprise Manager Administration Guide*.

15. Click the **Lock** icon to lock the fields you have configured. These fields cannot be edited once they are locked.
16. In the Schedule Deployment page, you can schedule the date on which the Java EE Application deployment procedure should be executed.
17. Click **Next**. On the Review page, review the details you have provided for the Deployment Procedure. If you are satisfied with the details, then click **Submit** to run the Deployment Procedure according to the schedule set. If you want to modify the details, click the Edit link in the section to be modified or click **Back** repeatedly to reach the page where you want to make the changes.

After you submit the deployment procedure, you will return to the Procedure Activity page where you can view the status of the Deployment Procedure. After the Java EE Application has been deployed, you can search for the target and navigate to the Target Home page.

17.5.3 Undeploying a Java EE Application

Follow these steps to undeploy a Java EE Application:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. Select the Java EE Application procedure from the list and click **Launch**. You can also use the following method to launch the deployment procedure:
 - Click **Middleware** from the Targets menu.
 - Right click on a WebLogic Domain from the list and from the context sensitive menu, select **Provisioning**, then select **Deploy / Undeploy Java EE Applications**.

- In the Deployment Procedure Manager page, select the Java EE Application Provisioning procedure and click **Launch**.
3. In the Select Targets page, choose the **Undeploy** operation.
4. Click **Add WLS Domains** to add one or more WebLogic domains. In the list of targets displayed, choose a target and click **Select**.
5. The deployment targets are listed in the Targets table. When an application is undeployed from the WebLogic domain, select the applications that need to be undeployed and click Next.
6. Click **Next**. Specify the credentials for each domain you have selected, the host on which the Administration Server is running, and the hosts to which the additional files or execution scripts are to be moved. You can choose:
 - Preferred Credentials: This option is selected by default and the preferred credentials stored in the Management Repository are used. This option is available only if it has already been defined in Cloud Control.
 - Named Credentials: A named credential specifies the authentication information for a user and can be a combination of username / password, public and private key pair, and can be used to perform provisioning, patching, run jobs, and other system management tasks.
 - New Credentials: You can override the preferred credentials and specify a separate set of credentials for each host and WebLogic domain being deployed.

For more information on setting up the credentials, see the *Enterprise Manager Security* chapter in the *Enterprise Manager Administration Guide*

7. Specify the deployment schedule and click **Next**.
8. Review the details and click **Undeploy**. You will return to the Procedure Activity page where you can check the status.

Provisioning Coherence Nodes and Clusters

This chapter explains how you can provision Coherence nodes or clusters across multiple targets in a farm using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Getting Started](#)
- [Supported Releases](#)
- [Deploying Coherence Nodes and Clusters](#)
- [Troubleshooting](#)

18.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in provisioning Coherence nodes and clusters. The Coherence Deployment Procedure allows you to do the following:

- Add one or more nodes to a new cluster and add this cluster as an Cloud Control monitored target.
- Add a management node to an existing cluster and add this cluster as an Cloud Control monitored target.
- Add one or more nodes to a cluster that is already being monitored by Cloud Control.
- Update existing nodes by copying modified software components or configuration files and restart the nodes.
- Create a new Coherence cluster.

Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully deploy a Coherence node. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 18–1 *Getting Started with Deploying a Coherence Node*

Step	Description	Reference Links
Step 1	<p>Understanding the Deployment Procedure</p> <p>Understand the Deployment Procedure that is offered by Cloud Control for deploying a Coherence node. Know how the Deployment Procedure functions, what use cases it covers, and so on.</p>	To learn about the Deployment Procedure, see Section 18.3 .

Table 18–1 (Cont.) Getting Started with Deploying a Coherence Node

Step	Description	Reference Links
Step 2	<p>Knowing About The Supported Releases</p> <p>Know what releases of Oracle Coherence are supported.</p>	To learn about the releases supported by the Deployment Procedure, see Section 18.2 .
Step 3	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as adding the Coherence node as a target, and setting up of Oracle Software Library.</p>	To learn about the prerequisites for deploying a Coherence node, see Section 18.3.1 .
Step 4	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully deploy a Coherence node.</p>	To deploy a Coherence node, follow the steps explained in Section 18.3.3 .

18.2 Supported Releases

This section lists the releases of Oracle Coherence supported by this Deployment Procedure:

- Oracle Coherence 3.3, 3.4, 3.5, 3.6, and 3.7.

18.3 Deploying Coherence Nodes and Clusters

This section describes how you can add one or more nodes to an existing cluster or create a new cluster using the Coherence Node Provisioning procedure.

This section covers the following:

- [Prerequisites](#)
- [Creating a Coherence Component](#)
- [Deployment Procedure](#)

18.3.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

- The host on which a Coherence node is being added or updated must be a monitored target in Cloud Control.
- A zip file with the Coherence software, default configuration files and start scripts must be created. This zip file must be added as a software component to the Oracle Software Library. If the size of the zip file is more than 2 MB, it must be uploaded from a host monitored by the Management Agent. You can add specific configuration files as components to the Software Library which will override the default configuration files. These configuration files can be different depending on the type of node (storage, management, etc.). While adding a software component, it is recommended that you specify the Product Name as **Coherence**.
- If you are provisioning a new node on a host on which the `coherence.jar` is not present, you must upload the `coherence.zip` file (containing Coherence software and default configuration files), and start scripts to the Oracle Software Library.

18.3.2 Creating a Coherence Component

You can create one or more Coherence components and save it to the Software Library. This components are required while provisioning Coherence nodes and clusters. To create a Coherence component, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. Create a folder in which the components are to be stored. After the folder has been created, select the folder and click **Create Entity** and **Component** from the Actions menu.
3. A Create Component popup window appears. From the Select Subtype drop down list, select the **Generic Component** and click **Continue**.

Figure 18–1 Create Generic Component: Describe Page

The screenshot shows the 'Software Library' interface for creating a generic component. The title is 'Create Generic Component: Describe'. Below the title, there are navigation buttons: 'Back', 'Step 1 of 3', 'Next', 'Save', and 'Cancel'. The page is divided into several sections:

- Name:** A text input field.
- Description:** A larger text area.
- Other Attributes:** A table with columns for 'Name' and 'Value'. There are three rows with empty fields.
- Attachments:** A section with a '+ Add' button and a table with columns for 'File Name', 'Size (KB)', and 'New Type'. A message below the table says 'No attachments have been added yet.'
- Notes:** A section with a '+ Add' button and a table with columns for 'Name', 'Added by', and 'Date'. A message below the table says 'No notes have been added yet.'

4. In the Create Generic Component: Describe page, enter the Product as Coherence. This is helpful when you are searching for files during Coherence Provisioning. Click **Next**.
5. In the Create Generic Component: Select Files page, check the **Upload Files** option.

Figure 18–2 Create Generic Component: Select Files Page

The screenshot shows the 'Software Library' interface for selecting files. The title is 'Create Generic Component: Select Files'. Below the title, there are navigation buttons: 'Back', 'Step 2 of 3', 'Next', 'Save', and 'Cancel'. The page is divided into several sections:

- Select one or more files to be associated with the entity:** A section with a message: 'Files can either be uploaded to or referred from a Software Library storage location.' There are two options: 'Upload Files' (selected) and 'Refer Files'.
- Specify Destination:** A section with a message: 'Choose a Software Library upload file storage location for uploading the specified files.' It includes fields for 'Upload Location', 'Storage Type', and 'Location Path'.
- Specify Source:** A section with a message: 'Files can be uploaded from either the local Resourcen or from a remote Resourcen monitored by an Enterprise Manager Agent. The Save and Upload action will submit a file transfer job for uploading the remote files to the specified upload location. For files uploaded from the local file system, the file size is limited to 2MB.' It includes a 'File Source' dropdown menu (set to 'Agent Machine') and a 'Host' text input field.

6. In the Specify Source section, select **Agent Machine** in the File Source drop down box and upload the following files:
 - `$AGENT_ROOT/plugins/oracle.sysman.emas.agent.plugin_12.1.0.1.0/archives/coherence/bulkoperationsmbean_11.1.1.jar`

- \$AGENT_ROOT/plugins/oracle.sysman.emas.agent.plugin_12.1.0.1.0/archives/coherence/coherenceEMIntg.jar
- \$AGENT_ROOT/plugins/oracle.sysman.emas.agent.plugin_12.1.0.1.0/scripts/coherence/default-start-script.pl

If you are uploading a large zip file such as Coherence.zip, you must save it on the Agent machine. Specify the path on the Agent to upload the file. This zip file must be downloaded from <http://www.oracle.com/technetwork/middleware/coherence/downloads/index.htm>

7. Click **Save and Upload** to submit a file transfer job to upload the remote files to the specified upload location.

18.3.3 Deployment Procedure

To deploy a Coherence node or a cluster, follow these steps:

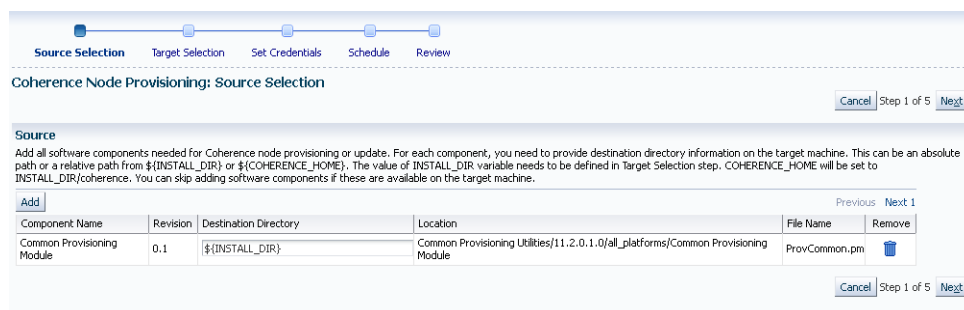
1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. Select the Coherence Node Provisioning deployment procedure and click **Launch**.

Note: You can also use the following methods to launch the deployment procedure:

- From the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**. Select the Coherence deployment procedure from the list and click **Launch**.
 - Select the **Coherence Node Provisioning** option from the Coherence Home page menu.
-

3. The Source Selection page which is the first page of the Coherence Node Provisioning wizard is displayed.

Figure 18–3 Source Selection Page



4. You can add all the software components needed to add or update a Coherence cluster. If the Coherence Home has already been created, you can click **Next** to go to the next page.

If the Coherence Home does not exist, click **Add** to add the Coherence binaries and the Start script from the Software Library. The Select Source popup is displayed. All software components with the product name Coherence that are

present in the Software Library are displayed. Select required components and click **Select**.

5. For each component you have selected, specify the destination directory on the target machine. This can be an absolute path or a relative path from `${INSTALL_DIR}` or `${COHERENCE_HOME}`. The contents of the `coherence.zip` file will be extracted to this directory.

Note:

- The value of the `$INSTALL_DIR` is defined in the Coherence Node Provisioning: Target Selection page and it is set as a level above the `COHERENCE_HOME` directory.
 - If the software components are available in the target machine, this step can be skipped.
-
-

6. Click **Next**. The Target Selection page is displayed. On this page, you can:
 - **Add Nodes:** You can add a new node or make a copy of an existing node. Click the **Search** icon in the Target Name field and select a Coherence cluster from the list. The following details are displayed:
 - **Cluster Name:** The name of the cluster.
 - **Cluster Communication:** This can be Multicast or Well Known Address (WKA).
 - **License Mode:** The mode in which the cluster has been deployed.

Click **Add** in the New Nodes section to add new nodes to an existing Coherence cluster monitored by Cloud Control. The Add Coherence Node page is displayed. Specify the details of the node and click **Continue** to add the node and return to the Coherence Node Provisioning: Select Target page. See [Section 18.3.3.1](#) for details.

- **Creating a Copy of an Existing Node:** You can make a copy of an existing node. When you select a cluster to which a node is to be added, a list of nodes present in the cluster are displayed in the Existing Nodes section. Select a node from this list and click **Create Like**. The Add Coherence Node page is displayed. Specify the details of the node and click **Continue** to return to the Coherence Node Provisioning: Select Target page. A copy of the selected node is now listed in the New Nodes section and can be deployed.
- **Create Cluster:** Click **Create Cluster** to create a new Coherence cluster. Enter Cluster Name along with the following details:
 - **Cluster Name:** Enter a unique name for the cluster.
 - **Cluster Communication:** Select **Multicast** or **Well Known Address (WKA)**. If you select Multicast, you are prompted for the Cluster Port and Cluster Address. If you select WKA, enter one or more sets of `<hostname>:<port>` entries separated by a comma and make sure that the WKA details have been specified in the Coherence Node Provisioning: Add Node page.

Note: If you select WKA, you need to create an override file (`tangosol-coherence-override-em.xml`) for the WKA entries and specify the `Dtangosol.coherence.override` parameter in this file. This file is created from the `default-start-script.pl` which can be modified if required.

- **License Mode:** Specify the mode in which the cluster is to be deployed. This can be Development, Evaluation, or Production.

Click **Add** in the New Nodes section to add nodes to the new cluster being created. The Add Coherence Node page is displayed. Specify the details of the node and click **Continue** to add the node and return to the Coherence Node Provisioning: Select Target page.

To create a cluster, you must have the following components, `coherenceEMIntg.jar`, `bulkoperationsmbean_11.1.1.jar`, `default-start-script.pl`, and `Coherence.zip`.

7. Click **Next** to go to the next step in the wizard. In the Coherence Node Provisioning: Set Credentials page, you can set credentials for each host. You can apply the same credentials for multiple hosts by selecting multiple hosts from the list.
8. Select the host and specify the credentials which can be:
 - **Preferred Credentials:** This option is selected by default and the preferred credentials stored in the Management Repository are used. This option is available only if it has already been defined in Cloud Control.
 - **Named Credentials:** You can override the preferred credentials and select a common set of credentials that will be used for all the hosts and WebLogic domains.
 - **New Credentials:** You can override the preferred credentials and specify a separate set of credentials for each host.

Select the credentials and click **Apply** to apply the credentials to the selected hosts. For more information on setting up credentials, see the Enterprise Manager Security chapter in the *Enterprise Manager Administration Guide*.

9. Click **Next**. The Schedule page is displayed. On this page, you can specify the schedule for deploying the node. You can choose to deploy the node immediately or at a later date.

Note: If you set the Grace Period as **Indefinite**, Cloud Control will keep trying to deploy the node for an indefinite period. If you specify a date / time in this field, the deployment process will be aborted after this period.

10. Click **Next**. The Review page is displayed. You can review the details you have provided for deploying the node. If you are updating a node, you can view the node processes that will be stopped on this page. Click **Finish** to deploy or update the node.

After the new Management Node has been created, you must wait for the first collection before you add nodes to the cluster.

18.3.3.1 Adding a Coherence Node

You can add a node to an existing cluster or create a new cluster by adding one or more new nodes. To add a node, follow these steps:

1. Click **Add** in the Coherence Node Provisioning: Target Selection page. The Add Coherence Node page is displayed. Enter the following details:

Figure 18–4 Add Coherence Node Page

Add Coherence Node

Host Details
 Select an EM Agent managed host where this Coherence node would be added. Enter required number of nodes on this host depending on the available resources. All nodes created Port values will be incremented by one from the entered value.
 * Host Name: Number of Nodes:

Node Details
 Provide node identification details.
 * Node Name: Site Name:
 Rack Name: Role Name:
 Unicast Address: Unicast Port:
 Well Known Address(WKA):
 Do not copy software components.

JVM Diagnostics Details
 Enter JVM Manager Host and JVM Manager Port to monitor this node using JVM
 JVM Manager Host: JVM Manager Port:

Management Node Details
 Select the Management node with MBeanServer checkbox and provide additional information. Only the primary management node is used for monitoring, but it is recommended to Select Primary management node for monitoring checkbox if this node is used for monitoring. Provide JMX user name and password if JMX authentication is enabled.
 Management node with MBeanServer
 * JMX Remote Port: JMX User Name:
 JMX Password:
 Use Bulk Operations MBean
Recommended for efficient monitoring.
 Primary management node used for monitoring

Environment Details
 Provide absolute paths to following home variables. Start script can be absolute path or relative to \${INSTALL_DIR}. COHERENCE_HOME is the full path to the INSTALL_DIR/coherence

Table 18–2 Add Coherence Node Page

Field Name	Description
Host Details	
Host Name	Select the host on which the node is to be added. You may have more than one node on the host depending on the machine configuration and the node configuration. Note: The Host Name you select here is used to set two start up parameters. Use the <code>tangosol_coherence_machine</code> environment variable to set the <code>tangosol.coherence.machine</code> parameter and <code>oracle_coherence_machine</code> to set the <code>oracle.coherence.machine</code> parameter.

Table 18–2 (Cont.) Add Coherence Node Page

Field Name	Description
Number of Nodes	<p>Specify the number of nodes that need to be added. By default, this field has the value of 1 but you can add as many nodes as required depending on the machine and node configuration. If the value is more than 1, then all the nodes will have the following properties:</p> <ul style="list-style-type: none"> Each node will use the same COHERENCE_HOME and start script. The Node Name value will be added as the prefix and a number will be appended to each node. For example <node_name>_1, <node_name>_2 and so on. Each name should be a unique one in the cluster. The JMX Remote Port value will be increased by 1 for each additional node. For example, if the value of the JMX Remote Port for the first node is 8088, the value for the second node will be 8089 and so on.
Node Details	
Node Name	Enter a unique name for the node
Site Name	This is the location of the Coherence node. This is geographical physical site name which identifies the racks and machines on which the node is running.
Rack Name	The name of the rack in the site on which the machine is located.
Role Name	<p>The role could be storage/data, application/process, proxy or management node.</p> <p>Note: The Node Name, Site Name, Rack Name, and Role Name cannot exceed 32 characters.</p>
Do not Copy Software Components	If you are adding a node on a machine on which a Coherence Home is already present, you must check the Do not copy Software Components checkbox. If you are copying the files onto a new host, unchecked the Do not copy Software Components checkbox to ensure that the binaries selected in the Coherence Node Provisioning: Source Selection page.
Well Known Address (WKA)	If Cluster Communication has been set to WKA in the Coherence Node Provisioning: Target Selection page, enter the host and port number in the format host1:port1, host2:port2 and so on.
JVM Diagnostics Details	
JVM Manager Host and Port	If this node is to be monitored by JVM Diagnostics Manager, specify the address and port number of the JVM Diagnostics Console.
Management Node Details	
Management Node with MBeanServer	You can define multiple management nodes in the cluster but only one management node can be marked as the Primary Management Node. We recommend that you add at least two management nodes preferably running on different hosts / machines to support fail over.
JMX Remote Port	The port number of the EMIntegration Mbean server.
JMX User Name	The user name for the JMX server if authentication is enabled.

Table 18–2 (Cont.) Add Coherence Node Page

Field Name	Description
JMX Password	The password for the JMX server if authentication is enabled. Note: To enable the JMX authentication, you need to set <code>com.sun.management.jmxremote.authenticate=true</code> . The JMX User name and JMX Password need to be set in the <code>\$JDK_HOME/jre/lib/management/jmxremote.password</code> and <code>\$JDK_HOME/jre/lib/management/jmxremote.access</code> files.
Primary Management Node used for Monitoring	Select this checkbox to mark the management node you are adding as the Primary Management Node used for Monitoring. This node is used to discover the Coherence cluster and any nodes added later will be added to the newly discovered cluster. If several nodes are being added to a cluster, only one management node can be marked as the primary one. If the primary management node fails, you can configure any of the other management nodes for monitoring. If no other management node is available, you can add a new primary management node to an existing cluster and this node can be used to monitoring.
Use Bulk Operations MBean	This checkbox is selected by default. When this option is selected, a new management node with BulkOperationsMBean will be started.
Environment Details	
Install Directory	Enter the absolute path to the folder under which the Coherence software components reside. The path specified here will be used as the Destination Directory specified on the Coherence Node Provisioning: Source Selection page. This value could be different for each node or the same for one or more nodes.
Start Script	This script is used to bring up the Coherence node. This script is operating system specific and sets the proper environment required for the node by specifying the relevant system parameters. See sample script for an example.

The following table summarizes how the values specified during deployment will be used by the environment variables specified in the start script. The deployment procedure also sets the `JAVA_HOME` and `AGENT_HOME` variables by using the Agent installation details. You may override these by specifying appropriate values in your start script.

Table 18–3 Environment Variables

UI Parameter	Environment Variable Set	Coherence System Parameter
CLUSTER_NAME	tangosol_coherence_cluster	tangosol.coherence.cluster
CLUSTER_ADDRESS	tangosol_coherence_clusteraddress	tangosol.coherence.clusteraddress
CLUSTER_PORT	tangosol_coherence_clusterport	tangosol.coherence.clusterport
NODE_NAME (32 chars)	tangosol_coherence_member	tangosol.coherence.member
SITE_NAME (32 chars)	tangosol_coherence_site	tangosol.coherence.site
RACK_NAME (32 chars)	tangosol_coherence_rack	tangosol.coherence.rack
MACHINE_NAME	tangosol_coherence_machine	tangosol.coherence.machine

Table 18–3 (Cont.) Environment Variables

UI Parameter	Environment Variable Set	Coherence System Parameter
ROLE_NAME (32 chars)	tangosol_coherence_role	tangosol.coherence.role
JMX_REMOTE_PORT	jmx_remote_port	com.sun.management.jmxremote.port
LICENSE_MODE	license_mode	tangosol.coherence.mode
COHERENCE_HOME	coherence_home	oracle.coherence.home
START_SCRIPT	start_script	oracle.coherence.startscript
JVM_CONSOLE_HOST	jvm_console_host	jamconhost
JVM_CONSOLE_PORT	jvm_console_port	jamconport
WKA_PORT	wka_port	tangosol.coherence.override=em-coherence-override.xml

2. After adding the node, click **Continue** to return to the Coherence Node Provisioning: Target Selection page.
3. Click **Next** to go to the next step in the wizard.

18.3.3.2 Sample Scripts

The `default-start-script.pl` and `generate-wka-override.pl` scripts are present in the `$EMAS_PLUGIN_ROOT/scripts/coherence/directory`.

18.3.3.2.1 default-start-script.pl

This script is the default start script used to start a Coherence node. A sample script is shown below:

```
#!/usr/local/bin/perl

# Sample script to demonstrate starting of following Coherence nodes.
# When this script is passed in as a start script in Coherence Node Provisioning
# Deployment Procedure, while executing start node step, the deployment procedure
# sets all user entered options as environment variables. Based on the values of
# these environment variables, you can start different types of Coherence nodes
#
# - Management Node with Oracle Bulk Operation MBean is started when
# "bulk_mbean" and "jmx_remote_port" variables are set. For this option,
# oracle.sysman.integration.coherence.EMIntegrationServer Java class is executed
# that starts a MBeanServer in this node and registers Oracle Bulk Operation
# MBean. You need coherenceEMIntg.jar and bulkoperationsmbean_11.1.1.jar in the
# classpath.
#
# - Management Node is started when "jmx_remote_port" is set, but "bulk_mbean" is
# NOT set.
#
# - Managed node when "jmx_remote_port" is not set.
#
# Following variables are set from the deployment procedure. Use these values to
# define required system parameters to override Coherence default settings.
```

```

my $coherence_home=$ENV{'COHERENCE_HOME'};

my $start_script=$ENV{'START_SCRIPT'};
my $java_home=$ENV{'JAVA_HOME'};
my $agent_home=$ENV{'AGENT_HOME'};
my $wka_port=$ENV{'WKA_PORT'};
my $license_mode=$ENV{'LICENSE_MODE'};
my $jamhost=$ENV{'JAM_CONSOLE_HOST'};
my $jampport=$ENV{'JAM_CONSOLE_PORT'};

my $member=$ENV{'tangosol_coherence_member'};
my $site=$ENV{'tangosol_coherence_site'};
my $rack=$ENV{'tangosol_coherence_rack'};
my $machine=$ENV{'tangosol_coherence_machine'};

# tangosol.coherence.machine has a limitation of 32 chars
# As a workaround, use oracle.coherence.machine to set machine name
# This parameter is used to identify hosts for cluster management features
my $oracle_coherence_machine=$ENV{'oracle_coherence_machine'};
my $role=$ENV{'tangosol_coherence_role'};

my $jmxport=$ENV{'jmx_remote_port'};
my $cluster=$ENV{'tangosol_coherence_cluster'};
my $clusteraddr=$ENV{'tangosol_coherence_clusteraddress'};
my $clusterport=$ENV{'tangosol_coherence_clusterport'};
my $bulkmbean=$ENV{'bulk_mbean'};
my $jmx_auth=$ENV{'jmx_enable_auth'};

my $SYS_OPT="";
my $JVM_OPT="";

my $psep="";
my $dsep="";
if ( !&IsWindows() ) {
    $psep=":";
    $dsep="/";
}
else
{
    $psep=";";
    $dsep="\"";
}

print
"\n\n*****\n"

print "Output from default-start-script\n";
print "Starting Node : $member\n";
print "Coherence Home : $coherence_home \n";
print "Start Script : $start_script \n";
print "Java Home : $java_home \n";
print "Agent Home : $agent_home \n";
print "WKA Port: $wka_port \n";
print "License Mode: $license_mode \n";

print "Site Name : $site \n";
print "Rack Name : $rack \n";
print "Machine Name : $machine \n";
print "Oracle Coherence Machine Name : $oracle_coherence_machine \n";

```

```

print "Role Name : $role \n";

print "Cluster Name : $cluster \n";
print "Cluster Addr : $clusteraddr \n";
print "Cluster Port : $clusterport \n";
print "JMX Port : $jmxport \n";
print "Bulk MBean : $bulkmbean \n";
print "JMX Auth Enabled : $jmx_auth \n";
#

# you may run a local script as part of this script and override those
# settings.
# Override JAVA_HOME variable by setting it locally
#
# ./set-env.sh
#echo "After setting JAVA_HOME locally, JAVA_HOME: $JAVA_HOME"
# Options for Java Virtual Machine.
$JVM_OPT="-server -Xms512m -Xmx512m -Xincgc -verbose:gc";
#
# Set system parameters to Coherence node
$SYS_OPT="-Djava.net.preferIPv4Stack=true";
# This param allows the mbeans on this node to be registered to mbean servers
running on management nodes

$SYS_OPT="$SYS_OPT -Dtangosol.coherence.management.remote=true";
$SYS_OPT="$SYS_OPT -Dcom.sun.management.jmxremote.ssl=false";
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.cluster=$cluster";
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.member=$member";
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.site=$site";
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.rack=$rack";
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.machine=$machine";
# set this if machine name > 32 chars, tangosol.coherence.machine has a limitaion
# of 32 chars
$SYS_OPT="$SYS_OPT -Doracle.coherence.machine=$oracle_coherence_machine";
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.role=$role";

# Set coh home and start script so they will be part of input args

$SYS_OPT="$SYS_OPT -Doracle.coherence.home=$coherence_home";
$SYS_OPT="$SYS_OPT -Doracle.coherence.startscript=$start_script";

# set jmxremote.authenticate=true if $jmx_enable_auth is present.
# username/password needs to be set in $JDK_
HOME/jre/lib/management/jmxremote.password and

# $JDK_HOME/jre/lib/management/jmxremote.access files.
Uncomment the following block after adding these files.
#
if ($jmx_auth ne "") {
$SYS_OPT="$SYS_OPT -Dcom.sun.management.jmxremote.authenticate=$jmx_auth";
  else {
$SYS_OPT="$SYS_OPT -Dcom.sun.management.jmxremote.authenticate=false";
}
}

# Default is true, so make sure to set it to false if not using authentication
# $SYS_OPT="$SYS_OPT -Dcom.sun.management.jmxremote.authenticate=false";
# set jmxremote.port only for management nodes, if user passes in.
# It enables monitoring from remote systems through this port.
if ($jmxport ne "") {

```

```

$SYS_OPT="$SYS_OPT -Dcom.sun.management.jmxremote.port=$jmxport";
}
#
# Define clusteraddress and clusterport if we have valid values.
#
if($clusteraddress ne "") {
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.clusteraddress=$clusteraddress";
}

if("$clusterport" ne "") {
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.clusterport=$clusterport";
}

if("$license_mode" ne "") {
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.mode=$license_mode";
}
#This is used to generate WKA override file. If you choose to use an existing
#override file, you can comment this out.
#Make sure you set "-Dtangosol.coherence.override" to the appropriate file name.
if("$wka_port" ne "") {
$wka_port = "\".$wka_port.\"";
$wka_script = $agent_
home.$dsep."sysman".$dsep."admin".$dsep."scripts".$dsep."coherence".$dsep."genera
te-wka-override.pl";
print "executing $wka_script $wka_port\n";
if ( !&IsWindows() ) {
system("chmod 0700 $wka_script");
}
if(fork() == 0) {
exec("$wka_script $wka_port") or die "Could not execute
generate-wka-override.xml\n";
}
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.override=em-coherence-override.xml";
}
my $startup_class="";
my $cmd="";
# Note that Coherence lib is under $COHERENCE_HOME/coherence. Add any application
# specific jars to this classpath, if needed.
my $CLASSPATH=$coherence_home.$dsep."lib".$dsep."coherence.jar".$psep.$coherence
_home.$dsep."lib".$dsep."reporter.jar";
print "CLASSPATH: $CLASSPATH\n";
if($jamhost ne "" && $jamport ne "") {
$CLASSPATH=$CLASSPATH.$psep.$agent
_home.$dsep."archives".$dsep."jlib".$dsep."jamagent.war";
my $jamjvmid="$cluster/$member";
print "Using Oracle JVMD - $jamjvmid\n";
$SYS_OPT="$SYS_OPT -Doracle.coherence.jamjvmid=$jamjvmid";
$SYS_OPT="jamconshost=$jamhost $SYS_OPT";
$SYS_OPT="jamconsport=$jamport $SYS_OPT";
$SYS_OPT=" oracle.ad4j.groupidprop=$jamjvmid $SYS_OPT";
}
if ($bulkmbean ne "" && $jmxport ne "") {
# Management node with Bulk Operation MBean.
# add Oracle supplied jars for Bulk Operation MBean
$CLASSPATH=$CLASSPATH.$psep.$agent
_home.$dsep."..".$dsep."..".$dsep."lib".$dsep."coherenceEMIntg.jar".$psep.$agent
_home.$dsep."..".$dsep."..".$dsep."dependencies".$dsep."bulkoperationsmbean
_11.1.1.jar";
# Start MBeanServer
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.management=all";

```

```

print "Starting a management node with Bulk Operation MBean \n";
$startup_class="oracle.sysman.integration.coherence.EMIntegrationServer";
$cmd=$java_home.$dsep."bin".$dsep."java -cp $CLASSPATH $JVM_OPT $SYS_OPT $startup
_class";
} elsif ($jmxport ne "") {
# Management Node with out Bulk Operation MBean
# Start MBeanServer
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.management=all";
print "Starting a management node ... \n";
$startup_class="com.tangosol.net.DefaultCacheServer";
$cmd=$java_home.$dsep."bin".$dsep."java -cp $CLASSPATH $JVM_OPT $SYS_OPT $startup
_class";
} else {
# A simple managed node. Do not start MBeanServer.
$SYS_OPT="$SYS_OPT -Dtangosol.coherence.management=none";
print "Starting a simple managed node ... \n";
$startup_class="com.tangosol.net.DefaultCacheServer";
$cmd=$java_home.$dsep."bin".$dsep."java -cp $CLASSPATH $JVM_OPT $SYS_OPT $startup
_class";
}
if ( !&IsWindows() ) {
if (fork() == 0) {
print "Executing start script from child process... $cmd \n";
exec("$cmd") or die "Could not execute $cmd\n";
}
} else {
print "Command used to start node = $cmd\n";
exec($cmd);
}
print "exiting default start script\n";
exit 0;
sub IsWindows {
$osname = $^O;
if ( $osname eq "Windows_NT"
|| $osname eq "MSWin32"
|| $osname eq "MSWin64" )
{
return 1;
}
else {
return 0;
}
}
}

```

18.3.3.2 generate-wka-override.pl

If Cluster Communication has been set to WKA in the Coherence Node Provisioning: Target Selection page, this script is launched by the default-start-script.pl. The generate-wka-override.pl is used to generate the override file. If you have your own override file, you can comment out the part that uses the generate-wka-override.pl script in the default-start-script.pl.

```

#!/usr/local/bin/perl
#
# $Header: emas/sysman/admin/scripts/coherence/generate-wka-override.pl /main/1
# 2011/02/01 16:51:33 $
#
# generate-wka-override.pl
#
# Copyright (c) 2011, 2011, Oracle and/or its affiliates. All rights reserved.

```

```

#
# NAME
# generate-wka-override.pl - <one-line expansion of the name>
#
# DESCRIPTION
# <short description of component this file declares/defines>
# expects input args as:
# host1:port1,host2:port2,host3:port3
# writes the wka information to em-coherence-override.xml
# Sample xml file:
#<coherence xml-override="/tangosol-coherence-override-{mode}.xml">
# <cluster-config>
# <unicast-listener>
# <well-known-addresses>
# <socket-address id="1">
# <address>10.232.129.69</address>
# <port>8088</port>
# </socket-address>
# <socket-address id="2">
# <address>10.232.129.69</address>
# <port>8089</port>
# </socket-address>
# </well-known-addresses>
# <port>8088</port>
# </unicast-listener>
# </cluster-config>
#</coherence>
#
use Cwd;
use IPC::Open3;
my $host_port = $ARGV[0];
@host_port_array = split(':', $host_port);
$size = @host_port_array;

my $xmlfile="em-coherence-override.xml";
print "$xmlfile\n";
open(XMLFL,"> $xmlfile");
print XMLFL "<coherence
xml-override=\"/tangosol-coherence-override-{mode}.xml\">\n";
print XMLFL "<cluster-config>\n";
print XMLFL "<unicast-listener>\n";
print XMLFL "<well-known-addresses>\n";

my $id = 1;
for($i = 0; $i < $size; $i++) {
$single_host_port = $host_port_array[$i];
$single_host_port =~ s/^\s+|\s+$//g;
@single_host_port_array = split(':', $single_host_port);
$wka_host = $single_host_port_array[0];
$wka_port = $single_host_port_array[1];
$id = $id + $i;
print XMLFL "<socket-address id=\"$id\">\n";
print XMLFL "<address>$wka_host</address>\n";
print XMLFL "<port>$wka_port</port>\n";
print XMLFL "</socket-address>\n";
}
print XMLFL "</well-known-addresses>\n";
print XMLFL "</unicast-listener>\n";
print XMLFL "</cluster-config>\n";
print XMLFL "</coherence>";

```

```
close(XMLFLL);  
exit 0;
```

18.4 Troubleshooting

We recommend that you have at least two management nodes running on different machines in a Coherence cluster. If a monitoring failure occurs, the second management node can be used. Some of the common failure scenarios are listed below:

- **Error Condition:** Loss of Management Node
Solution: If the primary management node fails, you need to change the monitoring configuration of the cluster to point to another management node in the cluster. If no other management node is present in the cluster, you can use the Coherence Node Provisioning deployment procedure, select an existing cluster and add a new management node. This process will update the monitoring configuration for the cluster.
- **Error Condition:** Loss of Agent Monitoring the Cluster
Solution: If the Agent is not available, you need to use another Management Agent to point to the management node of Coherence cluster.
- **Error Condition:** Loss of Host with EM Agent and Management Node
Solution: If the Host is not available, you need to switch to another management node that is running on a different machine.

Provisioning SOA Artifacts and Composites

This chapter explains how you can provision SOA Artifacts and Composites using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Understanding SOA Artifacts Provisioning](#)
- [Getting Started](#)
- [Deployment Procedures, Supported Releases, and Core Components Deployed](#)
- [Provisioning SOA Artifacts](#)
- [Deploying SOA Composites](#)

19.1 Understanding SOA Artifacts Provisioning

SOA artifacts deployment procedures support provisioning of SOA composites, Web Service policies, and policy and credential stores.

Following are some of the terms used in SOA artifacts provisioning:

SOA Composite

A SOA composite is a logical construct. Its components can run in a single process on a single computer or be distributed across multiple processes on multiple computers. A complete application might be constructed from just one composite, or it could combine several different composites. The components making up each composite might all use the same technology, or they might be built using different technologies.

SOA Infra Domain

The SOA Infrastructure domain is a WebLogic domain that contains soa-infra binaries. The SOA Infrastructure includes a set of service engines (BPEL process, human workflow, decision service, and Oracle mediator) that execute the business logic of their respective components within the SOA composite application (for example, a BPEL process).

Web Services

A Web service is a program that can be accessed remotely using different XML-based languages. What this program can do (that is, the functionality it implements) is described in a standard XML vocabulary called Web Services Description Language (WSDL). For example, a banking Web service may implement functions to check an account, print a statement, and deposit and withdraw funds. These functions are described in a WSDL file that any consumer can invoke to access the banking Web

service. As a result, a consumer does not have to know anything more about a Web service than the WSDL file that describes what it can do.

A Web service consumer (such as, a desktop application or a Java Platform, Enterprise Edition client such as a portlet) invokes a Web service by submitting a request in the form of an XML document to a Web service provider. The Web service provider processes the request and returns the result to the Web service consumer in an XML document.

WS Policies and Assertions

Policies describe the capabilities and requirements of a Web service such as whether and how a message must be secured, whether and how a message must be delivered reliably, and so on. Policies belong to one of the following categories: Reliable Messaging, Management, WS-Addressing, Security, and MTOM.

Policies are comprised of one or more assertions. A policy assertion is the smallest unit of a policy that performs a specific action. Policy assertions are executed on the request message and the response message, and the same set of assertions is executed on both types of messages. The assertions are executed in the order in which they appear in the policy. Assertions, like policies, belong to one of the following categories: Reliable Messaging, Management, WS-Addressing, Security, and MTOM.

Policy Stores

The Policy Store is a repository of system and application-specific policies and roles. Application roles can include enterprise users and groups specific to the application (such as administrative roles). A policy can use any of these groups or users as principals. A policy store can be file-based or LDAP-based. A file-based policy store is an XML file, and this store is the out-of-the-box policy store provider. An LDAP-based policy store can use either of the following LDAP servers: Oracle Internet Directory or Oracle Virtual Directory (with a local store adapter, or LSA).

Credential Stores

A Credential Store is a repository of security data (credentials) that certify the authority of users, Java components, and system components. A credential can hold user name and password combinations, tickets, or public key certificates. This data is used during authentication, when principals are populated in subjects, and, further, during authorization, when determining what actions the subject can perform.

19.2 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in provisioning SOA Artifacts and Composites. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision SOA Artifacts and Composites. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 19–1 Getting Started with Provisioning SOA Artifacts and Composites

Step	Description	Reference Links
Step 1	<p>Understanding the Deployment Procedure</p> <p>Understand the two Deployment Procedures that are offered by Cloud Control for provisioning SOA Artifacts and Composites. Know how the two Deployment Procedures function, what use cases they cover, what releases they support, and what core components they provision.</p>	To learn about the Deployment Procedure, see Section 19.3 .
Step 2	<p>Selecting the Deployment Procedure to Provision</p> <p>This chapter covers use cases for different SOA components. Identify the component you want to provision and understand the use cases that are covered.</p>	<ul style="list-style-type: none"> ■ To learn about provisioning SOA Artifacts, see Section 19.4. ■ To learn about provisioning SOA Composites, see Section 19.5.
Step 3	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	To learn about the prerequisites for provisioning SOA artifacts and composites, access the reference links provided for Step (2) and navigate to the <i>Prerequisites</i> subsection.
Step 4	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully provision SOA Artifacts and Composites.</p>	To provision SOA Artifacts and Composites, access the reference links provided for Step (2) and navigate to the <i>Provisioning Procedure</i> subsection.

19.3 Deployment Procedures, Supported Releases, and Core Components Deployed

Cloud Control offers the following Deployment Procedures for provisioning SOA Artifacts and Composites:

Deployment Procedure	Supported Releases	Artifacts Migrated
SOA Artifacts Provisioning	Oracle SOA Suite 11gR1 PS1 to PS4 (11.1.1.2.0) to 11.1.1.5.0)	<ul style="list-style-type: none"> ■ SOA Composites ■ Oracle WebLogic Server Policies ■ Assertion Templates ■ JPS Policy and Credential Stores
Deploy SOA Composites	Oracle SOA Suite 11gR1 PS1 to PS4 (11.1.1.2.0) to 11.1.1.5.0)	<ul style="list-style-type: none"> ■ SOA Composites

Note: Provisioning of a gold image from the Software Library is not supported for Microsoft Windows Vista.

Note: Cloning of human workflow artifacts and B2B artifacts are not supported. For information about cloning human workflow artifacts, see the *Oracle Fusion Middleware Administrator's Guide for Oracle SOA Suite and Oracle Business Process Management Suite*. For information about cloning B2B artifacts, see the *Oracle Fusion Middleware User's Guide for Oracle B2B*. These guides are available at:

http://download.oracle.com/docs/cd/E14571_01/index.htm

19.4 Provisioning SOA Artifacts

This section describes how you can provision SOA artifacts. In particular, this section covers the following:

- [Provisioning from a Reference Installation](#)
- [Provisioning SOA Artifacts from Gold Image](#)

19.4.1 Provisioning from a Reference Installation

This section describes how you can provision SOA artifacts from one soa-infra domain to another.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

19.4.1.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

- Ensure that you meet the prerequisites described in [Chapter 19](#).
- Ensure that you have already provisioned Oracle SOA Suite 11g and its underlying Oracle WebLogic Server Domain.
- Ensure that all the components (not only the soa-infra domain) within the source and target Oracle WebLogic Server Domains are up and running.
- Ensure that the source and the destination soa-infra domains are of the same version.

19.4.1.2 Provisioning Procedure

To provision SOA artifacts (composites, web service policies, JPS configuration) from a reference installation, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Deployment Procedure Manager page, in the Procedure Library subtab, from the table, select **SOA Artifacts Provisioning** deployment procedure. Select **Launch** and click **Go**. Cloud Control displays the Select Source page of the Deployment Procedure.

Note: You can also access this deployment procedure as follows:

- From the SOA Infrastructure Home page:
 1. From the Targets menu, click **Middleware**.
 2. In the Middleware page, click on a target of type **SOA Infrastructure**.
 3. In the SOA Infrastructure home page, from the SOA infrastructure-specific menu, select **SOA Artifacts Provisioning**.
-
-

3. On the Select Source page, do the following:
 - a. Retain the default selection, that is, **Provision from reference environment**.
 - b. Click on the torch icon against the **Domain Name** field. Search for the Oracle WebLogic Server Domain that you want to deploy the SOA artifacts from and select it. Ensure that the source Oracle WebLogic Server Domain is up and running.
 - c. In the **Credentials** section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. You are prompted to specify the Oracle WebLogic Server Domain credentials and the Oracle WebLogic Administration Server host credentials. In the Oracle WebLogic Server Domain Credentials section, specify the administrator credentials that can be used to access the WebLogic Server Administration Console. In the Oracle WebLogic Administration Server Host Credentials section, specify the operating system credentials of the user who installed the Admin Server.

- d. Optionally, if you want to save the SOA artifacts as an image in the Software Library, select **Save SOA Artifacts Gold Image in Software Library**.

For example, in future, if you want to provision this particular version to other Oracle WebLogic Server Domains, then instead of using the reference installation, which could potentially be down, you can use the gold image you saved in the Software Library.

- e. Click **Next**.
4. On the Select Destination page, do the following:
 - a. Click on the torch icon against the **Domain Name** field. Search for the Oracle WebLogic Server Domain that you want to deploy the SOA artifacts to and select it. Ensure that the destination Oracle WebLogic Server Domain is up and running.
 - b. In the **Credentials** section, retain the default selection, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. You are prompted to specify the Oracle WebLogic Server Domain credentials and the Oracle WebLogic Administration Server host credentials. In the Oracle WebLogic Server Domain Credentials section, specify the administrator credentials that can be

used to access the WebLogic Server Administration Console. In the Oracle WebLogic Administration Server Host Credentials section, specify the operating system credentials of the user who installed the Admin Server.

- c. Click **Next**.
5. On the Select Artifacts page, do the following:
 - a. In the **Choose the type of SOA artifacts to provision** section, select **SOA Composites, Web Services Policies, and Java Platform Security Configuration**.
 - b. Click **Next**.
6. On the SOA Composites page, do the following:
 - a. Select the composites you want to provision and specify a configuration plan from the Software Library or a directory.

It is recommended that you place the configuration plan in a directory on destination machine. Alternatively, you can also place the configuration plan in any other shared location which is accessible from the destination machine.

If the composite already exists on the destination host, then select **Overwrite** to overwrite that existing composite with the composite from the source domain.
 - b. Click **Next**.
7. On the Web Services Policies page, do the following:
 - a. In the Assertion Templates section, select the assertion templates to migrate.
 - b. In the Web Services Policies section, select the policies to migrate.
 - c. Click **Next**.
8. On the Java Platform Security page, do the following:
 - a. In the Migrate Policy Store and Credential Store section, select **Migrate Policy Store** and **Migrate Credential Store** check boxes.

To view a list of providers for the source and target, click **Provider details** link.
 - b. Click **Next**.
9. On the Schedule page, schedule the Deployment Procedure to run either immediately or later.
10. On the Review page, review the details you have provided for provisioning SOA artifacts, and click **Submit**.

19.4.2 Provisioning SOA Artifacts from Gold Image

This section describes how you can provision SOA artifacts (composites, web service policies, JPS configuration) from a gold image stored in the Software Library. In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

19.4.2.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Ensure that you have already provisioned Oracle SOA Suite 11g and its underlying Oracle WebLogic Server Domain.
- Ensure that the source and the destination soa-infra domains are of the same version.
- Ensure that you have already saved the gold image in the Software Library while provisioning the SOA artifacts from a reference installation.

19.4.2.2 Provisioning Procedure

To provision SOA artifacts from a gold image, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then click **Procedure Library**.
2. On the Deployment Procedure Manager page, in the Procedure Library subtab, from the table, select **SOA Artifacts Provisioning** deployment procedure. Select **Launch** and click **Go**. Cloud Control displays the Select Source page of the Deployment Procedure.

Note: You can also access this deployment procedure as follows:

- From the SOA Infrastructure Home page:
 1. From the Targets menu, click **Middleware**.
 2. In the Middleware page, click on a target of type **SOA Infrastructure**.
 3. In the SOA Infrastructure home page, from the SOA infrastructure-specific menu, select **SOA Artifacts Provisioning**.
-

3. On the Select Source page, do the following:
 - a. Select **Provision from Gold Image**.
 - b. Click on the torch icon against the **Gold Image Name** field. Search for the gold image you want to provision the SOA artifacts from and select it.
 - c. Click **Next**.
4. On the Select Destination page, do the following:
 - a. Click on the torch icon against the **Domain Name** field. Search for the Oracle WebLogic Server Domain that you want to deploy the SOA artifacts to and select it.
 - b. In the **Credentials** section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. You are prompted to specify the Oracle WebLogic Server Domain credentials and the Oracle WebLogic Administration Server host credentials. In the Oracle WebLogic Server Domain Credentials section, specify the administrator credentials that can be used to access the WebLogic Server Administration Console. In the Oracle

WebLogic Administration Server Host Credentials section, specify the operating system credentials of the user who installed the Admin Server.

- c. Click **Next**.
5. On the Select Artifacts page, do the following:
 - a. In the **Choose the type of SOA artifacts to provision** section, select **SOA Composites, Web Services Policies, and Java Platform Security Configuration**.
 - b. Click **Next**.
6. On the SOA Composites page, do the following:
 - a. Select the composites you want to provision and specify a configuration plan from the Software Library or a directory.
 If the composite already exists on the destination host, then select **Overwrite** to overwrite that existing composite with the composite from the source domain.
 - b. Click **Next**.
7. On the Web Services Policies page, do the following:
 - a. In the Assertion Templates section, select the assertion templates to migrate.
 - b. In the Web Services Policies section, select the policy assertions to migrate.
 - c. Click **Next**.
8. On the Java Platform Security page, do the following:
 - a. In the Migrate Policy Store and Credential Store section, select **Migrate Policy Store** and **Migrate Credential Store** check boxes.
 To view a list of providers for the target, click **Provider details** link.



- b. Click **Next**.
9. On the Schedule page, schedule the Deployment Procedure to run either immediately or later.
10. On the Review page, review the details you have provided for provisioning SOA artifacts, and click **Submit**.

19.5 Deploying SOA Composites

This section explains how you can deploy SOA composites. In particular, this section contains:

- [Prerequisites](#)
- [Provisioning Procedure](#)

19.5.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

- Ensure that you meet the prerequisites described in [Chapter 19](#).
- Ensure that you have already provisioned Oracle SOA Suite 11g and its underlying Oracle WebLogic Server Domain.
- Ensure that the source and the destination soa-infra domains are of the same version.

The domain should have at least one managed server with the SOA Infrastructure application running. In the case of a SOA Cluster, the composites will be deployed to any one managed server in the cluster.

- Ensure that you have the SOA Composites either in the Software Library or in a file system accessible from the Admin Server host.

19.5.2 Provisioning Procedure

To provision SOA composites, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Deployment Procedure Manager page, in the Procedure Library subtab, from the table, select **Deploy SOA Composites** deployment procedure. Select **Launch** and click **Go**. Cloud Control displays the Select Destination page of the Deployment Procedure.
3. On the Destination page, do the following:
 - a. Click on the torch icon against the **Destination Domain Name** field. Search for the Oracle WebLogic domain that you want to deploy the SOA composites to, and select it.
 - b. In the **Credentials** section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. You are prompted to specify the Oracle WebLogic Server Domain credentials and the Oracle WebLogic Administration Server host credentials. In the Oracle WebLogic Server Domain Credentials section, specify the administrator credentials that can be used to access the WebLogic Server Administration Console. In the Oracle WebLogic Administration Server Host Credentials section, specify the operating system credentials of the user who installed the Admin Server.

- c. Click **Next**.
4. On the Source page, do the following:
 - a. In the Composites section, click **Add**. Select Composites Source as Software Library or File System depending on where the composites are located. Select the Plan Source location and path.

If the composite already exists on the destination host, then select **Overwrite** to overwrite that existing composite with the composite from the source domain. If you want the composite that you are deploying now to be set as the default component, then retain the **Force Default** selection.

- b.** In the Options section, select **Verify adapter dependencies** if you want to ignore the missing adapters in the destination domain and proceed with the provisioning operation. Each composite may refer to one or more adapters, and the composites may not run properly if the depending adapters are missing in the destination domain. However, if you select this option, you can ignore all such missing adapters.
 - c.** Click **Next**.
- 5.** On the Schedule page, schedule the Deployment Procedure to run either immediately or later.
- 6.** On the Review page, review the details you have provided for provisioning SOA composites, and click **Submit**.

Provisioning Oracle Service Bus Resources

Oracle Service Bus is an enterprise-class service bus that connects, manages, and mediates interactions between heterogeneous services. Oracle Service Bus accelerates service configuration, integration, and deployment, thus simplifying management of shared services across the Service-Oriented Architecture (SOA).

The resources of Oracle Service Bus can be organized into individual projects. Projects are non-hierarchical, disjointed, top-level grouping constructs. All resources (such as business services, proxy services, WS-Policies, WSDLs, schemas, XQuery transformations, JARs, and so on) reside in exactly one non-overlapping project. Resources can be created directly under a project or be further organized into folders. Folders may be created inside projects or inside other folders, and the folders are similar to directories in a file system, with the project level being the root directory.

While Oracle Enterprise Manager Cloud Control (Cloud Control) allows you to discover and monitor these Oracle Service Bus targets, it also provides Deployment Procedures that help you provision Oracle Service Bus resources.

This chapter explains how you can provision Oracle Service Bus resources. In particular, this chapter covers the following:

- [Getting Started](#)
- [Deployment Procedure](#)
- [Supported Releases](#)
- [Provisioning Oracle Service Bus Resources from Oracle Service Bus Domain](#)
- [Provisioning Oracle Service Bus Resources from Oracle Software Library](#)

20.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in provisioning Oracle Service Bus resources. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision Oracle Service Bus resources. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 20–1 Getting Started with Provisioning Oracle Service Bus Resources

Step	Description	Reference Links
Step 1	<p>Understanding the Deployment Procedure</p> <p>Understand the Deployment Procedure that is offered by Cloud Control for provisioning Oracle Service Bus resources. Know how the Deployment Procedure functions, what use cases it covers, and so on.</p>	To learn about the Deployment Procedure, see Section 20.2 .
Step 2	<p>Knowing About The Supported Releases</p> <p>Know what releases of Oracle Service Bus can be provisioned by the Deployment Procedure.</p>	To learn about the releases supported by the Deployment Procedure, see Section 20.3 .
Step 3	<p>Selecting the Use Case</p> <p>This chapter covers a few use cases for provisioning Oracle Service Bus resources. Select the use case that best matches your requirement.</p>	<ul style="list-style-type: none"> ■ To learn about provisioning Oracle Service Bus resources from the an Oracle Service Bus domain, see Section 20.4. ■ To learn about provisioning Oracle Service Bus resources from the Software Library, see Section 20.5.
Step 4	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	<ul style="list-style-type: none"> ■ To learn about the prerequisites for provisioning Oracle Service Bus resources from the an Oracle Service Bus domain, see Section 20.4.1. ■ To learn the prerequisites for provisioning Oracle Service Bus resources from the Software Library, see Section 20.5.1.
Step 5	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully provision Oracle Service Bus resources.</p>	<ul style="list-style-type: none"> ■ To provision Oracle Service Bus resources from the an Oracle Service Bus domain, follow the steps explained in Section 20.4.2. ■ To provision Oracle Service Bus resources from the Software Library, follow the steps explained in Section 20.5.2.

20.2 Deployment Procedure

Cloud Control offers the following Deployment Procedure for provisioning Oracle Service Bus resources:

- *Oracle Service Bus Resource Provisioning*

20.3 Supported Releases

Using this Deployment Procedure, you can provision the resources for Oracle Service Bus 2.6, 2.6.1, 3.0, and 10gR3 (3.1).

20.4 Provisioning Oracle Service Bus Resources from Oracle Service Bus Domain

This section describes how you can provision Oracle Service Bus resources directly from an Oracle Service Bus domain.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

20.4.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Ensure that the source Oracle Service Bus (from where you want to export the resources) is already discovered and monitored in Cloud Control.
- If you want to use a customization file to customize the environment variables in the changed (target) environment, then you must ensure that the customization file is available as a generic component in Oracle Software Library. For instructions to create generic components, see [Section 2.2](#).

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as `mkdir`, `ls`, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Section 2.3.3](#).

20.4.2 Provisioning Procedure

To provision Oracle Service Bus resources from a source Oracle Service Bus domain, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. From the Deployment Procedures section, select the Oracle Service Bus Resource Provisioning procedure from the list and click **Launch**.
3. On the Select Source page, in the Source section, select **Oracle Service Bus Domain**.

Source
 Select a source where the resources to be deployed are available.

Oracle Service Bus Domain
Select a domain from where you want to export the resources

* Domain 

* BEA Home Directory

- a. For **Domain**, click the torch icon and select the Oracle Service Bus domain from where the resources can be exported and deployed to a target Oracle Service Bus domain. In the following page of the wizard, you will be allowed to select the domain's projects that you want to export.
 - b. For **BEA Home Directory**, specify the full path to the BEA home directory where all BEA product-related files are stored. For example, /home/mark/bea.
 - c. Click **Next**.
4. On the Select Projects page, do the following:
- a. In the Resource Summary section, select the projects you want to export and deploy to the target OSB domain. The selected projects are exported to a JAR file, and the JAR file is moved to the host where the target OSB domain is running.

Resource Summary: stapp04.us.oracle.com.servicebus_7021
 Select the projects that you want to export and deploy on the target Oracle Service Bus domain. The selected projects are exported to a JAR file and moved to the target host for deployment.

[Select All](#) | [Select None](#)

Select Project Name	Services
<input type="checkbox"/> HelloWorld	ProxyService/HelloWorld/ProxyServices/HelloWorldProxy BusinessService/HelloWorld/BusinessServices/HelloWorldBusinessService ProxyService/HelloWorld/testproxy/testproxy
<input type="checkbox"/> MortgageBroker	BusinessService/MortgageBroker/BusinessServices/normalLoanProcessor BusinessService/MortgageBroker/BusinessServices/managerLoanReviewService BusinessService/MortgageBroker/BusinessServices/loanSaleProcessor

Note that the resources of the selected projects that exist in the target OSB domain but not in the exported JAR file will be deleted.

- b. In the Export Mode section, do one of the following:
 Select **Export Projects** if you want to export the resources at project level. While deploying the exported JAR file to the target host, the entire project is deployed. This may add, overwrite, or delete resources depending on the availability of resources on the target host.
 Select **Export Resources** if you want to export the resources at resource level. While deploying the exported JAR file to the target host, only the resources are deployed. This may add or overwrite resources depending on the availability of resources on the target host.

Export Mode
 The resources of the selected projects can be exported at project level or resource level. If you export at project level, the resources of the selected projects that exist in the target Oracle Service Bus domain but not in the exported jar file will be deleted.

Export Projects
 Export Resources

To understand these options better, read the use cases described in [Section 20.4.2.1](#).

- c. (Optional) In the Security Options section, if the projects you want to export contain any resources with sensitive data, then specify a pass-phrase to protect them. The same pass-phrase will be used to import the protected resources during deployment.

Security Options

If the selected projects that you want to export contain any resources with sensitive data, then specify a pass phrase to protect those resources. The same pass phrase will be used to import the protected resources during deployment. Note that specifying pass phrase is optional.

Pass Phrase

- d. (Optional) In the Save Projects to Software Library section, select **Save Projects to Software Library** and specify a component name and location if you want to save the exported project JAR file as a generic component in the Software Library.

Save Projects to Software Library

By default, the selected projects are not saved during deployment. Use this option to upload the exported JAR file to the software library as a generic component. Review the name and location provided for the component.

Save Projects to Software Library

Component Name

Location

By default, the projects you select here are exported to a JAR file and moved to the host where the Administration server of the target Oracle Service Bus domain is running. However, the JAR files are not saved in the Software Library for future use. Using this option, you can save them as a component in the Software Library.

- 5. On the Select Target page, do the following:
 - a. In the Target section, specify the following:

For **Domain**, click the torch icon and select the Oracle Service Bus domain where you want to deploy the selected resources.

For **BEA Home Directory**, specify the full path to the BEA home directory where all BEA product-related files are stored.

Target

Select the Oracle Service Bus domain where you want to deploy the resources.

* Domain

* BEA Home Directory

- b. (Optional) In the Advanced Options section, select the settings you want to retain if you have done some customization to the resources selected for deployment, and if you want to preserve those changes in the target Oracle Service Bus domain.

Advanced Options

Preserve Environment Variables

Preserve Operational Values

Preserve Security and Policy Configuration

Preserve Credentials

Preserve Access Control Policies

TIP For OSB 2.6.x targets, Security and Policy cannot be preserved.

Note that for Oracle Service Bus 2.6.x, Security and Policy Configuration, Credentials, and Access Control Policies cannot be preserved.

- c. In the Customization section, provide details about the customization file that can be used to modify the environment settings in the target OSB domain.

Customization

Specify the location of a customization file available on the target host or Select a customization file from the Software Library. You can use customization files to make changes to environment values as well as to change references within resources. Note that using customization file is optional.

Customization File None

Use the customization file on the target host

Location

Specify the absolute path of the customization file on the target host

Use the customization file from the Software Library

Location

If you do not want to use a customization file, select **None**.

If you are using a customization file and if it is available on the host where the target OSB domain is running, then select **Use the Customization file on the target host** and specify the full path to the location where the file is present.

If the customization file is stored as a generic component in Oracle Software Library, then select **Select the customization file from the Software Library** and specify the full path to the location in Oracle Software Library where the generic component is stored.

- d. Click **Next**.
6. On the Set Credentials page, specify the following and click **Next**.
 - a. Specify the login credentials of the source and target Oracle Service Bus (OSB) domains.
 - b. Specify the credentials of the hosts where the Management Agents, which are monitoring the administration servers of the OSB domains, are running
7. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure to allow me to analyze results after performing prerequisite checks** to pause the procedure execution after all prerequisite checks are performed. Click **Next**.
8. On the Review page, review the details you have provided for the Deployment Procedure. If you are satisfied with the details, then click **Submit** to run the Deployment Procedure according to the schedule set. If you want to modify the details, click the **Edit** link in the section to be modified or click **Back** repeatedly to reach the page where you want to make the changes.
9. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the **Status** link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

20.4.2.1 Understanding Export Modes

The following describes the different use cases and explains how the export modes will work for those circumstances.

While the first column shows the project selected from the source domain and the resources contained in that selected project, the second column shows the availability of that project in the target domain. And, while the third column shows how Export at Project Level work, the fourth column shows how Export at Resource Level works.

Table 20–2 Understanding Export Modes

Source Domain	Target Domain	Export at Project Level	Export at Resource Level
You have selected Project_1 from the source domain, and this project has Resource_1, Resource_2, and Resource_3.	The target domain has no projects at all.	The entire Project_1 will be deployed to the target domain.	The entire Project_1 will be deployed to the target domain.
You have selected Project_1 from the source domain, and this project has Resource_1, Resource_2, and Resource_3.	The target domain has Project_1, and this project has Resource_1.	The entire Project_1 will be deployed to the target domain, wherein, Resource_1 will be overwritten because it is already available in the target domain, and Resource_2 and Resource_3 will be ADDED.	Only the resources of Project_1 will be deployed to the target domain, wherein, Resource_1 will be overwritten because it is already available in the target domain, and Resource_2 and Resource_3 will be ADDED.
You have selected Project_1 from the source domain, and this project has Resource_1.	The target domain has Project_1, and this project has Resource_1, Resource_2, and Resource_3.	The entire Project_1 will be deployed to the target domain, wherein, Resource_1 will be overwritten because it is already available in the target domain, and Resource_2 and Resource_3 will be DELETED.	Only the resources of Project_1 will be deployed to the target domain, wherein, only Resource_1 will be overwritten because it is already available in the target domain. The other two resources already available in the target domain, that is, Resource_2 and Resource_3 will NOT be affected.

20.5 Provisioning Oracle Service Bus Resources from Oracle Software Library

This section describes how you can provision Oracle Service Bus resources from the Software Library.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

20.5.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).

- Export the resources of an Oracle Service Bus domain as a JAR file. Use Oracle Service Bus console for this.
- Ensure that the JAR file is available as a generic component in Oracle Software Library. For instructions to create generic components, see [Section 2.2](#).
- If you want to use a customization file to customize the environment variables in the changed (target) environment, then you must ensure that the customization file is available as a generic component in Oracle Software Library. For instructions to create generic components, see [Section 2.2](#).

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as *mkdir*, *ls*, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

20.5.2 Provisioning Procedure

To provision Oracle Service Bus resources from a source Oracle Service Bus domain, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. From the Deployment Procedures section, select the Oracle Service Bus Resource Provisioning procedure from the list and click **Launch**.
3. On the Select Source page, in the Source section, select **Oracle Software Library**.
 - a. For **Component**, click the torch icon and select the generic component that contains the resources to be deployed to a target Oracle Service Bus domain.
 - b. (Optional) For **Pass Phrase**, specify a pass-phrase if any of the resources in the JAR file contain sensitive data and are protected. The same pass-phrase is used while importing these resources to the target domain.
 - c. Click **Next**. Cloud Control displays Select Target page.
4. On the Select Target page, do the following:
 - a. In the Target section, specify the following:

For **Domain**, click the torch icon and select the Oracle Service Bus domain where you want to deploy the selected resources.

For **BEA Home Directory**, specify the full path to the BEA home directory where all BEA product-related files are stored.

Target

Select the Oracle Service Bus domain where you want to deploy the resources.

• Domain 

• BEA Home Directory

- b. (Optional) In the Options section, select the settings you want to retain if you have done some customization to the resources selected for deployment, and if you want to preserve those changes in the target Oracle Service Bus domain.

Advanced Options

Preserve Environment Variables

Preserve Operational Values

Preserve Security and Policy Configuration

Preserve Credentials

Preserve Access Control Policies

TIP For OSB 2.6.x targets, Security and Policy cannot be preserved.

Note that for Oracle Service Bus 2.6.x, Security and Policy Configuration, Credentials, and Access Control Policies cannot be preserved.

- c. In the Customization section, provide details about the customization file that can be used to modify the environment settings in the target OSB domain.

Customization

Specify the location of a customization file available on the target host or Select a customization file from the Software Library. You can use customization files to make changes to environment values as well as to change references within resources. Note that using customization file is optional.


Customization File None

Use the customization file on the target host

Location

Specify the absolute path of the customization file on the target host

Use the customization file from the Software Library

Location 

If you do not want to use a customization file, select **None**.

If you are using a customization file and if it is available on the host where the target OSB domain is running, then select **Use the Customization file on the target host** and specify the full path to the location where the file is present.

If the customization file is stored as a generic component in Oracle Software Library, then select **Select the customization file from the Software Library** and specify the full path to the location in Oracle Software Library where the generic component is stored.

- d. Click **Next**.
5. On the Set Credentials page, specify the following and click **Next**.
- Specify the login credentials of the source and target Oracle Service Bus (OSB) domains.
 - Specify the credentials of the hosts where the Management Agents, which are monitoring the administration servers of the OSB domains, are running
6. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure to allow me to analyze**

results after performing prerequisite checks to pause the procedure execution after all prerequisite checks are performed. Click **Next**.

7. On the Review page, review the details you have provided for the Deployment Procedure. If you are satisfied with the details, then click **Submit** to run the Deployment Procedure according to the schedule set. If you want to modify the details, click the **Edit** link in the section to be modified or click **Back** repeatedly to reach the page where you want to make the changes.
8. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the **Status** link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

Provisioning Oracle BPEL Processes

Business Process Execution Language (BPEL) is an XML-based language for enabling task sharing across multiple enterprises using a combination of Web services. BPEL is based on the XML schema, simple object access protocol (SOAP), and Web services description language (WSDL). BPEL provides enterprises with an industry standard for business process orchestration and execution.

Oracle BPEL Process Manager (BPEL Process Manager) provides a framework for easily designing, deploying, monitoring, and administering processes based on BPEL standards.

While Oracle Enterprise Manager Cloud Control (Cloud Control) allows you to discover and monitor these BPEL Process Managers, it also provides Deployment Procedures that help you provision BPEL processes on BPEL Process Managers.

This chapter explains how you can provision BPEL processes on BPEL Process Managers. In particular, this chapter covers the following:

- [Getting Started](#)
- [Deployment Procedure](#)
- [Supported Releases](#)
- [Provisioning Oracle BPEL Processes](#)

21.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in provisioning Oracle BPEL processes. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision Oracle BPEL processes. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 21–1 *Getting Started with Provisioning Oracle BPEL Processes*

Step	Description	Reference Links
Step 1	<p>Understanding the Deployment Procedure</p> <p>Understand the Deployment Procedure that is offered by Cloud Control for provisioning Oracle BPEL processes. Know how the Deployment Procedure functions, what use cases it covers, and so on.</p>	To learn about the Deployment Procedure, see Section 21.2 .

Table 21–1 (Cont.) Getting Started with Provisioning Oracle BPEL Processes

Step	Description	Reference Links
Step 2	Knowing About The Supported Releases Know what releases of Oracle BPEL Process Manager are supported by the Deployment Procedure.	To learn about the releases supported by the Deployment Procedure, see Section 21.3 .
Step 3	Meeting the Prerequisites Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.	To learn about the prerequisites for provisioning Oracle BPEL processes, see Section 21.4.1 .
Step 4	Running the Deployment Procedure Run the Deployment Procedure to successfully provision Oracle BPEL processes.	To provision Oracle BPEL processes, follow the steps explained in Section 21.4.2 .

21.2 Deployment Procedure

Cloud Control offers the following Deployment Procedure for provisioning BPEL processes on BPEL Process Managers:

- [BPEL Process Provisioning](#)

21.3 Supported Releases

Using this Deployment Procedure, you can provision BPEL processes for Oracle BPEL Process Manager 10.1.3.1, 10.1.3.3, and 10.1.3.4.

21.4 Provisioning Oracle BPEL Processes

This section describes how you can provision BPEL processes for Oracle BPEL Process Manager.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

21.4.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Ensure that BPEL Process Manager on which the process suitcase files have to be deployed is already discovered and monitored in Cloud Control.
- Store the BPEL process suitcase files as generic components in the Software Library. For instructions to create generic components, see [Section 2.2](#).

Note: While adding a generic component for BPEL processes, on the Create Component: Describe page of the Software Library Wizard, select **Generic Component** from the **Type** list, provide a name for the parent folder, and navigate to the Upload File page to upload the files. You **DO NOT** have to provide details for Custom and Set Directives page.

- If you want to use a deployment plan that can be associated with a BPEL process suitcase file (JAR file), then store this deployment file as a generic component in the Software Library. For instructions to create generic components, see [Section 2.2](#).

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as *mkdir*, *ls*, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

21.4.2 Provisioning Procedure

To provision BPEL processes to a target BPEL Process Manager, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. From the Deployment Procedures section, select the BPEL Process Provisioning procedure from the list and click **Launch**.
3. On the Source Selection page, do the following:
 - a. In the Source section, click **Add** and select the BPEL Process suitcase files that you want to deploy to a target BPEL Process Manager. The table is populated based on the selection made.

Source
 Select the BPEL Process suitcase files that you want to deploy on Oracle BPEL Process Managers. The BPEL process suitcase files are BPEL process JAR files stored as generic components in Oracle Software Library.

Move Up Move Down **Add**

Select Name	Component Name	BPEL Process Name	Process Version	BPEL Suitcase Name	Component Location	Remove
<input checked="" type="checkbox"/>	Sample BPEL Suitcase	HelloWorld	1.0	bpel_HelloWorld_1.0.jar	Components/Oracle Components/BPEL Process Suitcase/Sample BPEL Suitcase	

TIP Use Move Up and Move Down to order the BPEL Process suitcases the way they should get be deployed on BPEL Process Manager

If you have selected multiple suitcase files, then from the table, select the BPEL process suitcase file and use **Move Up** and **Move Down** to order the components the way they should be deployed by the Deployment Procedure.

- b. In the Select Deployment Plan, select a deployment plan that can be associated with a BPEL process suitcase file (JAR file).

Select Deployment Plan
 Select a deployment plan for the BPEL suitcase that you want to associate to a bpel suitcase jar. A suitcase jar can contain a single deployment plan file called bpeldeployplan.xml. Deployment plan are stored as generic component in Oracle software library.

Select Deployment Plan

Component Location

TIP Functionality to associate a deployment plan to BPEL Process suitcase is limited to SOA 10.1.3.4 and subsequent SOA releases

The deployment plan helps you modify the configuration details and partner link binding properties, which have been set for a particular environment, at run time. You can also use it to search and replace strings and URLs that have been set for a particular environment. This way, you can deploy the same BPEL processes on BPEL Process Managers that are in development, test, and production environments; without having to reconfigure your settings across these environments.

- c. Click **Next**.
4. On the Target Selection page, in the Target section, click **Add** and select the BPEL Process Managers on which you want to deploy the BPEL processes. If there are multiple domains available for a BPEL target, then you can select an appropriate domain from the **BPEL Domain** list, on which the suitcase files can be deployed. Click **Next**.

Target
 Select Oracle BPEL Process Managers on which you want to deploy the selected BPEL Processes.

Add

BPEL Target Name	Host Name	BPEL Domain	Remove
soa_demo.stapp04.us.oracle.com_bpel	stapp04.us.oracle.com	default	

Note: When you click **Next**, Cloud Control internally checks to see if the Context Provider URL is captured. If this URL is not captured, then you may see some errors. To resolve this issue, set the URL in the Monitoring Configuration page of the BPEL target.

5. On the Credentials page, specify the following:

- a. Credentials of application server instances on which the selected BPEL Process Managers are running.

Application Server Credentials		
Provide credentials for the application server instances on which the selected Oracle BPEL Process Managers are running.		
Application Server	Username	Password
soa_demo.stapp04.us.oracle.com	<input type="text"/>	<input type="text"/>

- b. BPEL administrator credentials (and RMI credentials for 10.1.2 BPEL targets) for the selected Oracle BPEL Process Managers.

BPEL Process Manager Credentials		
Provide BPEL administrator credentials for the selected Oracle BPEL Process Managers.		
BPEL 10.1.3 Targets		
BPEL Process Manager	Username	Password
soa_demo.stapp04.us.oracle.com_bpel	<input type="text"/>	<input type="text"/>

The credentials required for BPEL Process Managers vary according to the supported BPEL Process Manager version. For BPEL 10.1.3 targets, you need to provide only one set of credentials that will be used for accessing the BPEL Process Manager. However, for BPEL 10.1.2 targets, you need to provide the BPEL administrator password and another set of OC4J RMI Access credentials for remote access.

If the preferred credentials are already set and stored in the Management Repository, then by default, they are prefilled on this page. You can choose to either use these prefilled preferred credentials or edit them to use the changed credentials. If the preferred credentials are not stored, then the fields are blank. In this case, you have to specify the credentials. The credentials specified here apply only to the current deployment procedure session and do not get stored in the Management Repository for future use.

Note that if you change the credentials, the change applies only to the current deployment procedure session and does not override the preferred credentials stored in the Management Repository.

- c. Click **Next**.
6. In the Schedule page, specify a Deployment Instance name. If you want to run the procedure immediately, then retain the default selection, that is, One Time (Immediately). If you want to run the procedure later, then select One Time (Later) and provide time zone, start date, and start time details. You can set the notification preferences according to deployment procedure status. If you want to run only prerequisites, you can select **Pause the procedure to allow me to analyze results after performing prerequisite checks** to pause the procedure execution after all prerequisite checks are performed. Click **Next**.
 7. On the Review page, review the details you have provided for the Deployment Procedure. If you are satisfied with the details, then click **Submit** to run the Deployment Procedure according to the schedule set. If you want to modify the details, click the **Edit** link in the section to be modified or click **Back** repeatedly to reach the page where you want to make the changes.
 8. In the Procedure Activity page, view the status of the execution of the job and steps in the deployment procedure. Click the **Status** link for each step to view the details of the execution of each step. You can click **Debug** to set the logging level to Debug and click **Stop** to stop the procedure execution.

Provisioning Oracle Application Server

This chapter explains how you can provision Oracle Application Servers using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Getting Started](#)
- [Deployment Procedures, Supported Releases, and Core Components Deployed](#)
- [Provisioning Oracle Application Server 10g Release 1 \(10.1.3\)](#)
- [Provisioning Oracle SOA Suite 10g \(10.1.3.4 and 10.1.3.5\)](#)

22.1 Getting Started

This section helps you get started with this chapter by providing an overview of the steps involved in provisioning Oracle Application Server. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision Oracle Application Server. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 22–1 *Getting Started with Provisioning Oracle Application Server*

Step	Description	Reference Links
Step 1	<p>Selecting the Release to Provision</p> <p>This chapter covers use cases for different releases of Oracle Application Server. Identify the release you want to provision and understand the use cases that are covered for each release.</p>	<ul style="list-style-type: none"> ■ To learn about provisioning Oracle Application Server 10g Release 1 (10.1.3), see Section 22.3. ■ To learn about provisioning Oracle SOA Suite 10g (10.1.3.x), see Section 22.4.
Step 2	<p>Meeting the Prerequisites</p> <p>Before you run any Deployment Procedure, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	To learn about the prerequisites for provisioning Oracle Application Server, access the reference links provided for Step (1) and navigate to the <i>Prerequisites</i> subsection.
Step 3	<p>Running the Deployment Procedure</p> <p>Run the Deployment Procedure to successfully provision Oracle Application Server.</p>	To provision Oracle Application Server, access the reference links provided for Step (1) and navigate to the <i>Provisioning Procedure</i> subsection.

22.2 Deployment Procedures, Supported Releases, and Core Components Deployed

Cloud Control offers the following Deployment Procedures for provisioning Oracle Application Server:

Deployment Procedure	Supported Releases	Core Components Deployed
Application Server Deployment 10.1.3	Oracle Application Server 10g Release 3 (10.1.3.4 and 10.1.3.5)	<ul style="list-style-type: none"> ■ Application tier ■ Web tier
Application Server Deployment 10.1.3.xSOA	Oracle SOA Suite 10g (10.1.3.4 and 10.1.3.5)	Deploys Oracle SOA Suite 10g (10.1.3.x) with the application tier and Web tier of Oracle Application Server 10g Release 3 (10.1.3.4 and 10.1.3.5)

Note: These Deployment Procedures do not install the database tier. However, they facilitate the configuration of Java Authentication and Authorization Service (JAAS) provider (also called as JAZN) with an existing data tier.

Oracle Application Server you want to provision may be available in different formats such as a running instance on a host monitored by Cloud Control, or a gold image in Oracle Software Library (Software Library).

Using the *Application Server Deployment 10.1.3* Deployment Procedure, you can provision any of these formats. However, if you want to have a copy of a running instance that is stable and has all the latest patches applied, the recommended option is to clone that existing instance so that you retain the same configuration settings. Similarly, if you have created a gold image of this stable, well-patched application server instance in the Software Library, then you can use it to deploy a similar instance in your enterprise configuration.

Note: Provisioning of a gold image from the Software Library is not supported for Microsoft Windows Vista.

22.3 Provisioning Oracle Application Server 10g Release 1 (10.1.3)

This section describes how you can provision Oracle Application Server 10g Release 1 (10.1.3). In particular, this section covers the following:

- [Cloning a Running Oracle Application Server Instance](#)
- [Provisioning a Gold Image of the Oracle Application Server](#)

22.3.1 Cloning a Running Oracle Application Server Instance

This section describes how you can clone an existing Oracle Application Server instance that is running on a host monitored by Cloud Control.

This option is best suited when you have a running instance of Oracle Application Server that is stable and has all the latest patches applied, and you want to make identical copies of it on multiple hosts.

However, the risk involved in using an existing instance is that the instance may be deleted or deinstalled anytime without prior notice, and as a result, the Deployment Procedure may fail. Therefore, use this option when you know that the running instance is available for cloning.

This section covers the following:

- [Cloning from an Existing Cluster, Scaling Up the Existing Cluster, and Using the Same Internet Directory](#)
- [Provisioning from an Existing Cluster and Creating a New Cluster Without Internet Directory](#)
- [Provisioning from an Existing Cluster and Creating a New Cluster With Internet Directory](#)

22.3.1.1 Cloning from an Existing Cluster, Scaling Up the Existing Cluster, and Using the Same Internet Directory

This section describes how you can provision the application tier and Web tier of Oracle Application Server 10g Release 1 (10.1.3) from an existing cluster, extend the cluster to include the new node, and by using the same Internet Directory.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

22.3.1.1.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Compare the configuration of the source and target hosts and ensure that they have the same configuration. If the configurations are different, then contact your system administrator and fix the inconsistencies before running the Deployment Procedure.

To compare the configuration of the hosts, in Cloud Control, click **Targets** and then **Hosts**. On the Hosts page, click the name of the source host to access its Home page, and then click the Configuration tab. On the Configuration page, click **Compare Configuration** and select the target host.

- If you are deploying multiple Web tiers, then ensure that a Software Load Balancer is set up and is accessible from the Web tier's hosts.

The Software Library provides a script to configure the F5 Big IP Application Switch (Software Version 4.5 PTF.5) load balancer on the selected Web tiers. For other systems such as Cisco CSM 3.1, overwrite the script with your specific configuration. The script is available in the following location of the Software Library:

Directives/Oracle Directives/Loadbalancer

- Ensure that the installation base directory, where the Web tier and application tier will be installed, is accessible (but not shared) on all target hosts.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as *mkdir*, *ls*, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

22.3.1.1.2 Provisioning Procedure

To provision a Web tier and an application tier, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. From the Deployment Procedures section, click **Application Server Provisioning Procedures**.
3. On the Deployment Procedure Manager page, in the Procedures subtab, from the table, select **Application Server Deployment 10.1.3**. Then click **Schedule Deployment**. Cloud Control displays the Source Selection page of the Deployment Procedure.
4. On the Source Selection page, in the Source Selection section, in the Select the source Oracle Homes from the Installed Cluster Environment subsection, do the following:
 - a. Retain the default selection, that is, **Select from Existing Cluster Installation**.
 - b. From the **Select Cluster** list, select an existing cluster from where the Web tier and application tier can be deployed. On selection of an existing cluster, the table gets populated with information about the Web tier and application tier that are part of it.
 - c. In the table, for **Files to Exclude**, specify the files in the Oracle home that you do not want to include while running this Deployment Procedure. You can specify either the file names or the file extensions, and separate multiple entries with a comma.

And for **Working Directory**, retain the default value or specify another location that already exists on the source host and can be used to stage the file for cloning.
 - d. If you want to deploy only one of the two products (application server or web server) from the selected source cluster, then click **Reset** to delete all values in the table. Once the values are reset, click the torch icon corresponding to the product that you want to deploy, and select the required target.
 - e. If you want to save the Oracle homes as an image in the Software Library, select **Save to Software Library**.

f. Click **Next**.

Note: When you click **Next**, if there are no prerequisites in the Software Library for that particular platform, then you will see **Next, Ignore Warnings** option. In this case, you can do one of the following:

- Upload the components to the Software Library under *Components/Oracle Components/Prerequisite-fixup components/<Platform name>/Prerequisite-Fixup component* and click **Next**.
 - Click **Next, Ignore Warnings** to skip the prerequisite check while running the Deployment Procedure.
-

5. On the Target List page, do the following:

- a. In the Web Tier Hosts section, click **Add** to add hosts on which you want to deploy the Web tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the application tier.
- b. In the Application Tier Hosts section, click **Add** to add hosts on which you want to deploy the application tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the Web tier.
- c. Click **Next**.

6. On the Credentials/Schedule page, do the following:

- a. In the Target Host Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- b. In the Agent Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

Note: You can optionally override these preferred credentials. The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- c. In the Source Oracle Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- d. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
 - e. Click **Next**.
7. On the Application and Web Tier page, do the following:

- a. In the Cluster Details section, retain the default selection, that is, **Extend existing cluster**.
- b. In the Instance Details section, retain the default instance names, and specify the OC4J administrator password for the source host and the target host.

You can always change the default instance names with any other custom names. However, ensure that the names you specify are unique because, by default, the host name and domain name of that host are appended to the instance name you specify here.

IMPORTANT:

- Each Oracle Application Server 10g instance has its own password, regardless of which user performed the installation. Passwords are not shared across instances, even if the instances were installed by the same user.
- If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in the Additional Parameters section. For more information, see Step 7 (e).
- The passwords you specify here must contain a minimum of 5 and a maximum of 30 alphanumeric characters. It can include underscore (`_`), dollar (`$`), or pound (`#`) characters. It must start with an alphabet and must contain at least one numeric value.

-
-
- c. In the Port Details section, retain the default port number (7777) that is displayed if Oracle Web Cache is not configured.
 - d. In the Load Balancer Details section, select **Configure Load Balancer** and provide the required information if you have an F5 BIG-IP Local Traffic Manager load balancer configured.

NOTE: Cloud Control supports only F5 BIG-IP Local Traffic Manager. If you have any other load balancer, then deselect **Configure Load Balancer**, and manually configure that load balancer and the HTTP servers associated with it. Do not use this section in this case.

- e. In the Additional Parameters section, specify any additional Web tier-specific or application tier-specific parameters you want to pass to the Deployment Procedure. For example, `-debug`. You can specify any other Oracle Universal Installer (OUI) parameter that can be in this provisioning operation.

IMPORTANT: If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in this section.

This is to ensure that the password you specify in the Instance Details section is uniformly propagated to all OC4J instances that are being provisioned.

However, if you still want to maintain different passwords for the provisioned OC4J instances, then after the deployment procedure ends successfully, access the application server console and change the passwords for the individual OC4J instances.

- f. In the Identify Management Configuration section, retain the default selection.
 - g. Click **Next**.
8. On the Configure Oracle Home page, do the following:
- a. If the hosts where the Web tier and application tier are being provisioned have a *direct* connection to the Internet, then specify an e-mail address and My Oracle Support password.

An e-mail address is required so that security updates and install updates can be sent. You can specify any e-mail address, but Oracle recommends you to specify the My Oracle Support user name. For example,
`john.mathew@xyz.com`.

If the My Oracle Support password is incorrect, you will be allowed two more attempts. However, if your password is incorrect in all three attempts or if it is left blank, then you are registered anonymously, which means, the configuration information will be collected and uploaded to My Oracle Support but the uploaded information will not be associated with your My Oracle Support account. Therefore, if you log in to My Oracle Support with your credentials, you will not see this information displayed against your account. However, if you had specified an e-mail address, then you will continue to receive security updates and other notifications from Oracle to that e-mail address.

- b. If the hosts where the Web tier and application tier are being provisioned have an *indirect* connection to the Internet through a proxy server, then specify an e-mail address and My Oracle Support password, and then in the Connection Details section, specify the proxy server details.

Note: You can change the proxy server settings any time after the Deployment Procedure ends. To do so, run the `configCCR` command from the `/ccr/bin/` directory within the Oracle home directory of the provisioned application server.

- c. If the hosts where the Web tier and application tier are being provisioned do not have a *direct* or *indirect* connection to the Internet, then specify the e-mail address and leave the other fields blank.

In this case, after you complete the installation process, manually collect the configuration information and upload it to My Oracle Support.

- d. Click **Next**.
9. On the Review page, review the details you have provided for provisioning a Web tier and application tier, and click **Submit**.

22.3.1.2 Provisioning from an Existing Cluster and Creating a New Cluster Without Internet Directory

This section describes how you can provision the application tier and Web tier of Oracle Application Server 10g Release 1 (10.1.3) from an existing cluster, and create a new cluster without Internet directory.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

22.3.1.2.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Compare the configuration of the source and target hosts and ensure that they have the same configuration. If the configurations are different, then contact your system administrator and fix the inconsistencies before running the Deployment Procedure.

To compare the configuration of the hosts, in Cloud Control, click **Targets** and then **Hosts**. On the Hosts page, click the name of the source host to access its Home page, and then click the Configuration tab. On the Configuration page, click **Compare Configuration** and select the target host.

- If you are deploying multiple Web tiers, then ensure that a Software Load Balancer is set up and is accessible from the Web tier's hosts.

The Software Library provides a script to configure the F5 Big IP Application Switch (Software Version 4.5 PTF.5) load balancer on the selected Web tiers. For other systems such as Cisco CSM 3.1, overwrite the script with your specific configuration. The script is available in the following location of the Software Library:

```
Directives/Oracle Directives/Loadbalancer
```

- Ensure that the installation base directory, where the Web tier and application tier will be installed, is accessible (but not shared) on all target hosts.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as *mkdir*, *ls*, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

22.3.1.2.2 Provisioning Procedure

To provision a Web tier and an application tier, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. From the Deployment Procedures section, click **Application Server Provisioning Procedures**.
3. On the Deployment Procedure Manager page, in the Procedures subtab, from the table, select **Application Server Deployment 10.1.3**. Then click **Schedule Deployment**.
4. On the Source Selection page, in the Source Selection section, in the Select the source Oracle Homes from the Installed Cluster Environment subsection, do the following:
 - a. Retain the default selection, that is, **Select from Existing Cluster Installation**.
 - b. From the **Select Cluster** list, select an existing cluster from where the Web tier and application tier can be deployed. On selection of an existing cluster, the table gets populated with information about the Web tier and application tier that are part of it
 - c. In the table, for **Files to Exclude**, specify the files in the Oracle home that you do not want to include while running this Deployment Procedure. You can specify either the file names or the file extensions, and separate multiple entries with a comma.

And for **Working Directory**, retain the default value or specify another location that already exists on the source host and can be used to stage the file for cloning.
 - d. If you want to deploy only one of the two products (application server or web server) from the selected source cluster, then click **Reset** to delete all values in the table. Once the values are reset, click the torch icon corresponding to the product that you want to deploy, and select the required target.
 - e. If you want to save the Oracle homes as an image in the Software Library, select **Save to Software Library**.
 - f. Click **Next**.

5. On the Target List page, do the following:
 - a. In the Web Tier Hosts section, click **Add** to add hosts on which you want to deploy the Web tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the application tier.
 - b. In the Application Tier Hosts section, click **Add** to add hosts on which you want to deploy the application tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the Web tier.
 - c. Click **Next**.
6. On the Credentials/Schedule page, do the following:
 - a. In the Target Host Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

Note: You can optionally override these preferred credentials. The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- b. In the Agent Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- c. In the Source Oracle Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make,

specify the credentials. Ensure that the users belong to the same operating system group.

- d. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
 - e. Click **Next**.
7. On the Application and Web Tier page, do the following:
- a. In the Cluster Details section, select **Create new Cluster**. By default, Cloud Control prefills the details based on an existing cluster. You can either use the default values or specify a new cluster name, installation directory, and multicast address and port. Also ensure that the multicast address and port are different from the ones configured for the source cluster.

For **Web Tier Install Base Directory** and **Application Tier Install Base Directory**, ensure that you specify the absolute path to the directory where you want to deploy the Web tier and application tier, respectively.

For **Multicast Address**, ensure that the address is within the range of 224.0.0.0 and 239.255.255.255. This is a single IP address for a set of nodes that are joined in a multicasting group.

- b. In the Instance Details section, specify unique instance names for the Web tier instance and application tier instance, and specify the OC4J administrator password for the source host and the target host.

You can always change the default instance names with any other custom names. However, ensure that the names you specify are unique because, by default, the host name and domain name of that host are appended to the instance name you specify here.

IMPORTANT:

- Each Oracle Application Server 10g instance has its own password, regardless of which user performed the installation. Passwords are not shared across instances, even if the instances were installed by the same user.
 - If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in the Additional Parameters section. For more information, see Step 7 (e).
 - The passwords you specify here must contain a minimum of 5 and a maximum of 30 alphanumeric characters. It can include underscore (`_`), dollar (`$`), or pound (`#`) characters. It must start with an alphabet and must contain at least one numeric value.
-
-

- c. In the Port Details section, specify the HTTP load balancer host and listener ports to manage HTTP connections made by client applications. Alternatively, you can retain the default value, that is, 7777. Select **Enable SSL** if you want to secure the communications.
- d. In the Load Balancer Details section, select **Configure Load Balancer** and provide the required information if you have an F5 BIG-IP Local Traffic Manager load balancer configured.

NOTE: Cloud Control supports only F5 BIG-IP Local Traffic Manager. If you have any other load balancer, then deselect **Configure Load Balancer**, and manually configure that load balancer and the HTTP servers associated with it. Do not use this section in this case.

- e. In the Additional Parameters section, specify any additional Web tier-specific or application tier-specific parameters you want to pass to the Deployment Procedure. For example, `-debug`. You can specify any other Oracle Universal Installer (OUI) parameter that can be in this provisioning operation.

IMPORTANT: If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in this section.

This is to ensure that the password you specify in the Instance Details section is uniformly propagated to all OC4J instances that are being provisioned.

However, if you still want to maintain different passwords for the provisioned OC4J instances, then after the deployment procedure ends successfully, access the application server console and change the passwords for the individual OC4J instances.

- f. In the Identify Management Configuration section, select **None**.
 - g. Click **Next**.
8. On the Configure Oracle Home page, do the following:
- a. If the hosts where the Web tier and application tier are being provisioned have a *direct* connection to the Internet, then specify an e-mail address and My Oracle Support password.

An e-mail address is required so that security updates and install updates can be sent. You can specify any e-mail address, but Oracle recommends you to specify the My Oracle Support user name. For example,
`john.mathew@xyz.com`.

If the My Oracle Support password is incorrect, you will be allowed two more attempts. However, if your password is incorrect in all three attempts or if it is left blank, then you are registered anonymously, which means, the configuration information will be collected and uploaded to My Oracle Support but the uploaded information will not be associated with your My Oracle Support account. Therefore, if you log in to My Oracle Support with your credentials, you will not see this information displayed against your account. However, if you had specified an e-mail address, then you will continue to receive security updates and other notifications from Oracle to that e-mail address.
 - b. If the hosts where the Web tier and application tier are being provisioned have an *indirect* connection to the Internet through a proxy server, then specify an e-mail address and My Oracle Support password, and then in the Connection Details section, specify the proxy server details.

Note: You can change the proxy server settings any time after the Deployment Procedure ends. To do so, run the `configCCR` command from the `/ccr/bin/` directory within the Oracle home directory of the provisioned application server.

- c. If the hosts where the Web tier and application tier are being provisioned do not have a *direct* or *indirect* connection to the Internet, then specify the e-mail address and leave the other fields blank.

In this case, after you complete the installation process, manually collect the configuration information and upload it to My Oracle Support.

- d. Click **Next**.
9. On the Review page, review the details you have provided for provisioning a Web tier and application tier, and click **Submit**.

22.3.1.3 Provisioning from an Existing Cluster and Creating a New Cluster With Internet Directory

This section describes how you can provision the application tier and Web tier of Oracle Application Server 10g Release 1 (10.1.3) from an existing cluster, and create a new cluster with Internet directory.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

22.3.1.3.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Compare the configuration of the source and target hosts and ensure that they have the same configuration. If the configurations are different, then contact your system administrator and fix the inconsistencies before running the Deployment Procedure.

To compare the configuration of the hosts, in Cloud Control, click **Targets** and then **Hosts**. On the Hosts page, click the name of the source host to access its Home page, and then click the Configuration tab. On the Configuration page, click **Compare Configuration** and select the target host.

- If you are deploying multiple Web tiers, then ensure that a Software Load Balancer is set up and is accessible from the Web tier's hosts.

The Software Library provides a script to configure the F5 Big IP Application Switch (Software Version 4.5 PTF.5) load balancer on the selected Web tiers. For other systems such as Cisco CSM 3.1, overwrite the script with your specific configuration. The script is available in the following location of the Software Library:

Directives/Oracle Directives/Loadbalancer

- Ensure that the installation base directory, where the Web tier and application tier will be installed, is accessible (but not shared) on all target hosts.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as *mkdir*, *ls*, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

22.3.1.3.2 Provisioning Procedure

To provision a Web tier and an application tier, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. From the Deployment Procedures section, click **Application Server Provisioning Procedures**.
3. On the Deployment Procedure Manager page, in the Procedures subtab, from the table, select **Application Server Deployment 10.1.3**. Then click **Schedule Deployment**.
4. On the Source Selection page, in the Source Selection section, in the Select the source Oracle Homes from the Installed Cluster Environment subsection, do the following:
 - a. Retain the default selection, that is, **Select from Existing Cluster Installation**.
 - b. From the **Select Cluster** list, select an existing cluster from where the Web tier and application tier can be deployed. On selection of an existing cluster, the table gets populated with information about the Web tier and application tier that are part of it
 - c. In the table, for **Files to Exclude**, specify the files in the Oracle home that you do not want to include while running this Deployment Procedure. You can specify either the file names or the file extensions, and separate multiple entries with a comma.

And for **Working Directory**, retain the default value or specify another location that already exists on the source host and can be used to stage the file for cloning.
 - d. If you want to deploy only one of the two products (application server or web server) from the selected source cluster, then click **Reset** to delete all values in the table. Once the values are reset, click the torch icon corresponding to the product that you want to deploy, and select the required target.
 - e. If you want to save the Oracle homes as an image in the Software Library, select **Save to Software Library**.
 - f. Click **Next**. Cloud Control displays the Target List page.

5. On the Target List page, do the following:
 - a. In the Web Tier Hosts section, click **Add** to add hosts on which you want to deploy the Web tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the application tier.
 - b. In the Application Tier Hosts section, click **Add** to add hosts on which you want to deploy the application tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the Web tier.
 - c. Click **Next**.
6. On the Credentials/Schedule page, do the following:
 - a. In the Target Host Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

Note: You can optionally override these preferred credentials. The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- b. In the Agent Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- c. In the Source Oracle Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make,

specify the credentials. Ensure that the users belong to the same operating system group.

- d. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
7. On the Application and Web Tier page, do the following:
- a. In the Cluster Details section, select **Create new Cluster**. By default, Cloud Control prefills the details based on an existing cluster. You can either use the default values or specify a new cluster name, installation directory, and multicast address and port. Also ensure that the multicast address and port are different from the ones configured for the source cluster.

For **Web Tier Install Base Directory** and **Application Tier Install Base Directory**, ensure that you specify the absolute path to the directory where you want to deploy the Web tier and application tier, respectively.

For **Multicast Address**, ensure that the address is within the range of 224.0.0.0 and 239.255.255.255. This is a single IP address for a set of nodes that are joined in a multicasting group.

- b. In the Instance Details section, specify unique instance names for the Web tier instance and application tier instance, and specify the OC4J administrator password for the source host and the target host.

You can always change the default instance names with any other custom names. However, ensure that the names you specify are unique because, by default, the host name and domain name of that host are appended to the instance name you specify here.

IMPORTANT:

- Each Oracle Application Server 10g instance has its own password, regardless of which user performed the installation. Passwords are not shared across instances, even if the instances were installed by the same user.
- If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in the Additional Parameters section. For more information, see Step 7 (e).
- The passwords you specify here must contain a minimum of 5 and a maximum of 30 alphanumeric characters. It can include underscore (`_`), dollar (`$`), or pound (`#`) characters. It must start with an alphabet and must contain at least one numeric value.

-
-
- c. In the Port Details section, specify the HTTP load balancer host and listener ports to manage HTTP connections made by client applications. Alternatively, you can retain the default value, that is, 7777. Select **Enable SSL** if you want to secure the communications.
 - d. In the Load Balancer Details section, select **Configure Load Balancer** and provide the required information if you have an F5 BIG-IP Local Traffic Manager load balancer configured.

NOTE: Cloud Control supports only F5 BIG-IP Local Traffic Manager. If you have any other load balancer, then deselect **Configure Load Balancer**, and manually configure that load balancer and the HTTP servers associated with it. Do not use this section in this case.

- e. In the Additional Parameters section, specify any additional Web tier-specific or application tier-specific parameters you want to pass to the Deployment Procedure. For example, `-debug`. You can specify any other Oracle Universal Installer (OUI) parameter that can be in this provisioning operation.

IMPORTANT: If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in this section.

This is to ensure that the password you specify in the Instance Details section is uniformly propagated to all OC4J instances that are being provisioned.

However, if you still want to maintain different passwords for the provisioned OC4J instances, then after the deployment procedure ends successfully, access the application server console and change the passwords for the individual OC4J instances.

- f. In the Identify Management Configuration section, select **Configure Java Authentication and Authorization Service (JAZN) with a LDAP-based provider**.

Using this option, you can set up JAZN LDAP-based provider for authentication and authorization for OC4J application.

Java Authentication and Authorization Service (JAAS) is a Java package that enables services and applications to authenticate and enforce access controls upon users. Oracle Application Server 10g Containers for J2EE (OC4J) supports JAAS by implementing a JAAS provider (also called as JAZN).

The JAAS provider provides application developers with user authentication, authorization, and delegation services to integrate into their application environments. It also supports JAAS policies. Policies contain the rules (permissions) that authorize a user to use resources, such as reading a file and so on.

- g. Click **Next**. Cloud Control displays the Identity Management page.
- 8. On the Identity Management page, do the following:
 - a. In the Identity Management Host Details section, specify the connection information for the Internet Directory to be used for Identity Management of the Oracle Application Server users and groups. If you do not have an Internet Directory installed, install it using the OracleAS Infrastructure component.
 - b. In the Internet Directory Login Details section, specify credentials of the user who belongs to the iASAdmin group in the Internet Directory.
 - c. Click **Next**. Cloud Control displays the Configure Oracle Home page.
 - 9. On the Configure Oracle Home page, do the following:

- a. If the hosts where the Web tier and application tier are being provisioned have a *direct* connection to the Internet, then specify an e-mail address and My Oracle Support password.

An e-mail address is required so that security updates and install updates can be sent. You can specify any e-mail address, but Oracle recommends you to specify the My Oracle Support user name. For example, john.mathew@xyz.com.

If the My Oracle Support password is incorrect, you will be allowed two more attempts. However, if your password is incorrect in all three attempts or if it is left blank, then you are registered anonymously, which means, the configuration information will be collected and uploaded to My Oracle Support but the uploaded information will not be associated with your My Oracle Support account. Therefore, if you log in to My Oracle Support with your credentials, you will not see this information displayed against your account. However, if you had specified an e-mail address, then you will continue to receive security updates and other notifications from Oracle to that e-mail address.

- b. If the hosts where the Web tier and application tier are being provisioned have an *indirect* connection to the Internet through a proxy server, then specify an e-mail address and My Oracle Support password, and then in the Connection Details section, specify the proxy server details.

Note: You can change the proxy server settings any time after the Deployment Procedure ends. To do so, run the `configCCR` command from the `/ccr/bin/` directory within the Oracle home directory of the provisioned application server.

- c. If the hosts where the Web tier and application tier are being provisioned do not have a *direct* or *indirect* connection to the Internet, then specify the e-mail address and leave the other fields blank.

In this case, after you complete the installation process, manually collect the configuration information and upload it to My Oracle Support.

10. On the Review page, review the details you have provided for provisioning a Web tier and application tier, and click **Submit**.

22.3.2 Provisioning a Gold Image of the Oracle Application Server

This section describes how you can provision a gold image of Oracle Application Server. In particular, this section covers the following:

- [Provisioning and Creating a New Cluster Without Internet Directory](#)
- [Provisioning and Creating a New Cluster With Internet Directory](#)
- [Provisioning and Treating Oracle Application Server as a Standalone Instance Without Internet Directory](#)
- [Provisioning and Treating Oracle Application Server as a Standalone Instance With Internet Directory](#)

22.3.2.1 Provisioning and Creating a New Cluster Without Internet Directory

This section describes how you can provision the application tier and Web tier of Oracle Application Server 10g Release 1 (10.1.3), which are identical to the ones

available on a gold image available in the Software Library, and create a new cluster without Internet directory.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

22.3.2.1.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Compare the configuration of the source and target hosts and ensure that they have the same configuration. If the configurations are different, then contact your system administrator and fix the inconsistencies before running the Deployment Procedure.

To compare the configuration of the hosts, in Cloud Control, click **Targets** and then **Hosts**. On the Hosts page, click the name of the source host to access its Home page, and then click the Configuration tab. On the Configuration page, click **Compare Configuration** and select the target host.

- If you are deploying multiple Web tiers, then ensure that a Software Load Balancer is set up and is accessible from the Web tier's hosts.

The Software Library provides a script to configure the F5 Big IP Application Switch (Software Version 4.5 PTF.5) load balancer on the selected Web tiers. For other systems such as Cisco CSM 3.1, overwrite the script with your specific configuration. The script is available in the following location of the Software Library:

```
Directives/Oracle Directives/Loadbalancer
```

- Ensure that the installation base directory, where the Web tier and application tier will be installed, is accessible (but not shared) on all target hosts.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as `mkdir`, `ls`, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

22.3.2.1.2 Provisioning Procedure

To provision a Web tier and an application tier, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. In Deployment Procedures section, click **Application Server Provisioning Procedures**.
3. On the Deployment Procedure Manager page, in the Procedures subtab, from the table, select **Application Server Deployment 10.1.3**. Then click **Schedule Deployment**.
4. On the Source Selection page, in the Source Selection section, in the Select the Gold Image of an Oracle Home or a shiphome from the Software Library subsection, do the following:
 - a. Select **Select from Software Library**.
 - b. In the **Source for Web Tier** section, click the torch icon and select the generic component that contains the Web tier.
 - c. In the **Source for App Tier** section, click the torch icon and select the generic component that contains the application tier.

Note: When you click the torch icon to search for components, the Select Component page displays the components available in the Software Library.

- If you want to deploy a fresh installation, then select the shiphome component that is in "Ready" status. By default, the Select Component page does not display components with "Active" status.
 - If you want to deploy a gold image, then select the gold image component that is either in "Ready" or "Active" status.
-
-

- d. Click **Next**.
5. On the Target List page, do the following:
 - a. In the Web Tier Hosts section, click **Add** to add hosts on which you want to deploy the Web tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the application tier.
 - b. In the Application Tier Hosts section, click **Add** to add hosts on which you want to deploy the application tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the Web tier.
 - c. Click **Next**.
6. On the Credentials/Schedule page, do the following:
 - a. In the Target Host Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make,

specify the credentials. Ensure that the users belong to the same operating system group.

- b. In the Agent Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

Note: You can optionally override these preferred credentials. The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- c. In the Source Oracle Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- d. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
- e. Click **Next**.

- 7. On the Application and Web Tier page, do the following:

- a. In the Cluster Details section, select **Create new Cluster**. By default, Cloud Control prefills the details based on an existing cluster. You can either use the default values or specify a new cluster name, installation directory, and multicast address and port. Also ensure that the multicast address and port are different from the ones configured for the source cluster.

For **Web Tier Install Base Directory** and **Application Tier Install Base Directory**, ensure that you specify the absolute path to the directory where you want to deploy the Web tier and application tier, respectively.

For **Multicast Address**, ensure that the address is within the range of 224.0.0.0 and 239.255.255.255. This is a single IP address for a set of nodes that are joined in a multicasting group.

- b. In the Instance Details section, specify unique instance names for the Web tier instance and application tier instance, and specify the OC4J administrator password for the source host and the target host.

You can always change the default instance names with any other custom names. However, ensure that the names you specify are unique because, by default, the host name and domain name of that host are appended to the instance name you specify here.

IMPORTANT:

- Each Oracle Application Server 10g instance has its own password, regardless of which user performed the installation. Passwords are not shared across instances, even if the instances were installed by the same user.
- If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in the Additional Parameters section. For more information, see Step 7 (e).
- The passwords you specify here must contain a minimum of 5 and a maximum of 30 alphanumeric characters. It can include underscore (`_`), dollar (`$`), or pound (`#`) characters. It must start with an alphabet and must contain at least one numeric value.

-
-
- c. In the Port Details section, specify the HTTP load balancer host and listener ports to manage HTTP connections made by client applications. Alternatively, you can retain the default value, that is, 7777. Select **Enable SSL** if you want to secure the communications.
- d. In the Load Balancer Details section, select **Configure Load Balancer** and provide the required information if you have an F5 BIG-IP Local Traffic Manager load balancer configured.

NOTE: Cloud Control supports only F5 BIG-IP Local Traffic Manager. If you have any other load balancer, then deselect **Configure Load Balancer**, and manually configure that load balancer and the HTTP servers associated with it. Do not use this section in this case.

- e. In the Additional Parameters section, specify any additional Web tier-specific or application tier-specific parameters you want to pass to the Deployment Procedure. For example, `-debug`. You can specify any other Oracle Universal Installer (OUI) parameter that can be in this provisioning operation.

IMPORTANT: If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in this section.

This is to ensure that the password you specify in the Instance Details section is uniformly propagated to all OC4J instances that are being provisioned.

However, if you still want to maintain different passwords for the provisioned OC4J instances, then after the deployment procedure ends successfully, access the application server console and change the passwords for the individual OC4J instances.

- f. In the Identify Management Configuration section, select **None**.
 - g. Click **Next**.
8. On the Configure Oracle Home page, do the following:
- a. If the hosts where the Web tier and application tier are being provisioned have a *direct* connection to the Internet, then specify an e-mail address and My Oracle Support password.

An e-mail address is required so that security updates and install updates can be sent. You can specify any e-mail address, but Oracle recommends you to specify the My Oracle Support user name. For example,
john.mathew@xyz.com.

If the My Oracle Support password is incorrect, you will be allowed two more attempts. However, if your password is incorrect in all three attempts or if it is left blank, then you are registered anonymously, which means, the configuration information will be collected and uploaded to My Oracle Support but the uploaded information will not be associated with your My Oracle Support account. Therefore, if you log in to My Oracle Support with your credentials, you will not see this information displayed against your account. However, if you had specified an e-mail address, then you will continue to receive security updates and other notifications from Oracle to that e-mail address.

- b. If the hosts where the Web tier and application tier are being provisioned have an *indirect* connection to the Internet through a proxy server, then specify an e-mail address and My Oracle Support password, and then in the Connection Details section, specify the proxy server details.

Note: You can change the proxy server settings any time after the Deployment Procedure ends. To do so, run the `configCCR` command from the `/ccr/bin/` directory within the Oracle home directory of the provisioned application server.

- c. If the hosts where the Web tier and application tier are being provisioned do not have a *direct* or *indirect* connection to the Internet, then specify the e-mail address and leave the other fields blank.

In this case, after you complete the installation process, manually collect the configuration information and upload it to My Oracle Support.

- d. Click **Next**.

9. On the Review page, review the details you have provided for provisioning a Web tier and application tier, and click **Submit**.

22.3.2.2 Provisioning and Creating a New Cluster With Internet Directory

This section describes how you can provision the application tier and Web tier of Oracle Application Server 10g Release 1 (10.1.3), which are identical to the ones available on a gold image present in the Software Library, and create a new cluster with Internet directory.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

22.3.2.2.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Compare the configuration of the source and target hosts and ensure that they have the same configuration. If the configurations are different, then contact your system administrator and fix the inconsistencies before running the Deployment Procedure.

To compare the configuration of the hosts, in Cloud Control, click **Targets** and then **Hosts**. On the Hosts page, click the name of the source host to access its Home page, and then click the Configuration tab. On the Configuration page, click **Compare Configuration** and select the target host.

- If you are deploying multiple Web tiers, then ensure that a Software Load Balancer is set up and is accessible from the Web tier's hosts.

The Software Library provides a script to configure the F5 Big IP Application Switch (Software Version 4.5 PTF.5) load balancer on the selected Web tiers. For other systems such as Cisco CSM 3.1, overwrite the script with your specific configuration. The script is available in the following location of the Software Library:

```
Directives/Oracle Directives/Loadbalancer
```

- Ensure that the installation base directory, where the Web tier and application tier will be installed, is accessible (but not shared) on all target hosts.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as `mkdir`, `ls`, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

22.3.2.2.2 Provisioning Procedure

To provision a Web tier and an application tier, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. In the Deployment Procedures section, click **Application Server Provisioning Procedures**.
3. On the Deployment Procedure Manager page, in the Procedures subtab, from the table, select **Application Server Deployment 10.1.3**. Then click **Schedule Deployment**.
4. On the Source Selection page, in the Source Selection section, in the Select the Gold Image of an Oracle Home from the Software Library subsection, do the following:
 - a. Select **Select from Software Library**.
 - b. In the **Source for Web Tier** section, click the torch icon and select the generic component that contains the Web tier.
 - c. In the **Source for App Tier** section, click the torch icon and select the generic component that contains the application tier.

Note: When you click the torch icon to search for components, the Select Component page displays the components available in the Software Library. If you want to deploy a gold image, then select the gold image component that is either in **Ready** or **Active** status.

- d. Click **Next**.
5. On the Target List page, do the following:
 - a. In the Web Tier Hosts section, click **Add** to add hosts on which you want to deploy the Web tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the application tier.
 - b. In the Application Tier Hosts section, click **Add** to add hosts on which you want to deploy the application tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the Web tier.
 - c. Click **Next**.
6. On the Credentials/Schedule page, do the following:
 - a. In the Target Host Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

Note: You can optionally override these preferred credentials. The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- b. In the Agent Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- c. In the Source Oracle Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- d. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
- e. Click **Next**.

7. On the Application and Web Tier page, do the following:

- a. In the Cluster Details section, select **Create new Cluster**. By default, Cloud Control prefills the details based on an existing cluster. You can either use the default values or specify a new cluster name, installation directory, and multicast address and port. Also ensure that the multicast address and port are different from the ones configured for the source cluster.

For **Web Tier Install Base Directory** and **Application Tier Install Base Directory**, ensure that you specify the absolute path to the directory where you want to deploy the Web tier and application tier, respectively.

For **Multicast Address**, ensure that the address is within the range of 224.0.0.0 and 239.255.255.255. This is a single IP address for a set of nodes that are joined in a multicasting group.

- b. In the Instance Details section, specify unique instance names for the Web tier instance and application tier instance, and specify the OC4J administrator password for the source host and the target host.

You can always change the default instance names with any other custom names. However, ensure that the names you specify are unique because, by default, the host name and domain name of that host are appended to the instance name you specify here.

IMPORTANT:

- Each Oracle Application Server 10g instance has its own password, regardless of which user performed the installation. Passwords are not shared across instances, even if the instances were installed by the same user.
- If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in the Additional Parameters section. For more information, see Step 7 (e).
- The passwords you specify here must contain a minimum of 5 and a maximum of 30 alphanumeric characters. It can include underscore (`_`), dollar (`$`), or pound (`#`) characters. It must start with an alphabet and must contain at least one numeric value.

-
-
- c. In the Port Details section, specify the HTTP load balancer host and listener ports to manage HTTP connections made by client applications. Alternatively, you can retain the default value, that is, 7777. Select **Enable SSL** if you want to secure the communications.
 - d. In the Load Balancer Details section, select **Configure Load Balancer** and provide the required information if you have an F5 BIG-IP Local Traffic Manager load balancer configured.

NOTE: Cloud Control supports only F5 BIG-IP Local Traffic Manager. If you have any other load balancer, then deselect **Configure Load Balancer**, and manually configure that load balancer and the HTTP servers associated with it. Do not use this section in this case.

- e. In the Additional Parameters section, specify any additional Web tier-specific or application tier-specific parameters you want to pass to the Deployment Procedure. For example, `-debug`. You can specify any other Oracle Universal Installer (OUI) parameter that can be in this provisioning operation.

IMPORTANT: If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in this section.

This is to ensure that the password you specify in the Instance Details section is uniformly propagated to all OC4J instances that are being provisioned.

However, if you still want to maintain different passwords for the provisioned OC4J instances, then after the deployment procedure ends successfully, access the application server console and change the passwords for the individual OC4J instances.

- f. In the Identify Management Configuration section, select **Configure Java Authentication and Authorization Service (JAZN) with a LDAP-based provider**.

Using this option, you can set up JAZN LDAP-based provider for authentication and authorization for OC4J application.

Java Authentication and Authorization Service (JAAS) is a Java package that enables services and applications to authenticate and enforce access controls upon users. Oracle Application Server 10g Containers for e (OC4J) supports JAAS by implementing a JAAS provider (also called as JAZN).

The JAAS provider provides application developers with user authentication, authorization, and delegation services to integrate into their application environments. It also supports JAAS policies. Policies contain the rules (permissions) that authorize a user to use resources, such as reading a file and so on.

- g. Click **Next**.

8. On the Identity Management page, do the following:

- a. In the Identity Management Host Details section, specify the connection information for the Internet Directory to be used for Identity Management of the Oracle Application Server users and groups. If you do not have an Internet Directory installed, install it using the OracleAS Infrastructure component.
- b. In the Internet Directory Login Details section, specify credentials of the user who belongs to the iASAdmin group in the Internet Directory.
- c. Click **Next**.

9. On the Configure Oracle Home page, do the following:

- a. If the hosts where the Web tier and application tier are being provisioned have a *direct* connection to the Internet, then specify an e-mail address and My Oracle Support password.

An e-mail address is required so that security updates and install updates can be sent. You can specify any e-mail address, but Oracle recommends you to specify the My Oracle Support user name. For example, `john.mathew@xyz.com`.

If the My Oracle Support password is incorrect, you will be allowed two more attempts. However, if your password is incorrect in all three attempts or if it is left blank, then you are registered anonymously, which means, the configuration information will be collected and uploaded to My Oracle Support but the uploaded information will not be associated with your My

Oracle Support account. Therefore, if you log in to My Oracle Support with your credentials, you will not see this information displayed against your account. However, if you had specified an e-mail address, then you will continue to receive security updates and other notifications from Oracle to that e-mail address.

- b. If the hosts where the Web tier and application tier are being provisioned have an *indirect* connection to the Internet through a proxy server, then specify an e-mail address and My Oracle Support password, and then in the Connection Details section, specify the proxy server details.

Note: You can change the proxy server settings any time after the Deployment Procedure ends. To do so, run the `configCCR` command from the `/ccr/bin/` directory within the Oracle home directory of the provisioned application server.

- c. If the hosts where the Web tier and application tier are being provisioned do not have a *direct* or *indirect* connection to the Internet, then specify the e-mail address and leave the other fields blank.

In this case, after you complete the installation process, manually collect the configuration information and upload it to My Oracle Support.

- d. Click **Next**.

10. On the Review page, review the details you have provided for provisioning a Web tier and application tier, and click **Submit**.

22.3.2.3 Provisioning and Treating Oracle Application Server as a Standalone Instance Without Internet Directory

This section describes how you can provision the application tier and Web tier of Oracle Application Server 10g Release 1 (10.1.3), which are identical to the ones available on a gold image available in the Software Library, and treat that as a standalone instance without Internet directory.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

22.3.2.3.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Compare the configuration of the source and target hosts and ensure that they have the same configuration. If the configurations are different, then contact your system administrator and fix the inconsistencies before running the Deployment Procedure.

To compare the configuration of the hosts, in Cloud Control, click **Targets** and then **Hosts**. On the Hosts page, click the name of the source host to access its Home page, and then click the Configuration tab. On the Configuration page, click **Compare Configuration** and select the target host.

- If you are deploying multiple Web tiers, then ensure that a Software Load Balancer is set up and is accessible from the Web tier's hosts.

The Software Library provides a script to configure the F5 Big IP Application Switch (Software Version 4.5 PTF.5) load balancer on the selected Web tiers. For other systems such as Cisco CSM 3.1, overwrite the script with your specific configuration. The script is available in the following location of the Software Library:

Directives/Oracle Directives/Loadbalancer

- Ensure that the installation base directory, where the Web tier and application tier will be installed, is accessible (but not shared) on all target hosts.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as *mkdir*, *ls*, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

22.3.2.3.2 Provisioning Procedure

To provision a Web tier and an application tier, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. In Deployment Procedures section, click **Application Server Provisioning Procedures**.
3. On the Deployment Procedure Manager page, in the Procedures subtab, from the table, select **Application Server Deployment 10.1.3**. Then click **Schedule Deployment**.
4. On the Source Selection page, in the Source Selection section, in the Select the Gold Image of an Oracle Home from the Software Library subsection, do the following:
 - a. Select **Select from Software Library**.
 - b. In the **Source for Web Tier** section, click the torch icon and select the generic component that contains the Web tier.
 - c. In the **Source for App Tier** section, click the torch icon and select the generic component that contains the application tier.

Note: When you click the torch icon to search for components, the Select Component page displays the components available in the Software Library. If you want to deploy a gold image, then select the gold image component that is either in **Ready** or **Active** status.

- d. Click **Next**.
5. On the Target List page, do the following:
 - a. In the Web Tier Hosts section, click **Add** to add hosts on which you want to deploy the Web tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the application tier.
 - b. In the Application Tier Hosts section, click **Add** to add hosts on which you want to deploy the application tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the Web tier.
 - c. Click **Next**.
 6. On the Credentials/Schedule page, do the following:
 - a. In the Target Host Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

Note: You can optionally override these preferred credentials. The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- b. In the Agent Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- c. In the Source Oracle Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- d. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
 - e. Click **Next**.
7. On the Application and Web Tier page, do the following:
 - a. In the Cluster Details section, select **Standalone AS**.
 - b. In the Instance Details section, specify unique instance names for the Web tier instance and application tier instance, and specify the OC4J administrator password for the source host and the target host.

You can always change the default instance names with any other custom names. However, ensure that the names you specify are unique because, by default, the host name and domain name of that host are appended to the instance name you specify here.

IMPORTANT:

- Each Oracle Application Server 10g instance has its own password, regardless of which user performed the installation. Passwords are not shared across instances, even if the instances were installed by the same user.
- If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in the Additional Parameters section. For more information, see Step 7 (e).
- The passwords you specify here must contain a minimum of 5 and a maximum of 30 alphanumeric characters. It can include underscore (`_`), dollar (`$`), or pound (`#`) characters. It must start with an alphabet and must contain at least one numeric value.

-
-
- c. In the Port Details section, specify the HTTP load balancer host and listener ports to manage HTTP connections made by client applications. Alternatively, you can retain the default value, that is, 7777. Select **Enable SSL** if you want to secure the communications.
 - d. In the Load Balancer Details section, select **Configure Load Balancer** and provide the required information if you have an F5 BIG-IP Local Traffic Manager load balancer configured.

NOTE: Cloud Control supports only F5 BIG-IP Local Traffic Manager. If you have any other load balancer, then deselect **Configure Load Balancer**, and manually configure that load balancer and the HTTP servers associated with it. Do not use this section in this case.

- e. In the Additional Parameters section, specify any additional Web tier-specific or application tier-specific parameters you want to pass to the Deployment Procedure. For example, `-debug`. You can specify any other Oracle Universal Installer (OUI) parameter that can be in this provisioning operation.

IMPORTANT: If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in this section.

This is to ensure that the password you specify in the Instance Details section is uniformly propagated to all OC4J instances that are being provisioned.

However, if you still want to maintain different passwords for the provisioned OC4J instances, then after the deployment procedure ends successfully, access the application server console and change the passwords for the individual OC4J instances.

- f. In the Identify Management Configuration section, select **None**.
 - g. Click **Next**.
8. On the Configure Oracle Home page, do the following:
- a. If the hosts where the Web tier and application tier are being provisioned have a *direct* connection to the Internet, then specify an e-mail address and My Oracle Support password.

An e-mail address is required so that security updates and install updates can be sent. You can specify any e-mail address, but Oracle recommends you to specify the My Oracle Support user name. For example,
`john.mathew@xyz.com`.

If the My Oracle Support password is incorrect, you will be allowed two more attempts. However, if your password is incorrect in all three attempts or if it is left blank, then you are registered anonymously, which means, the configuration information will be collected and uploaded to My Oracle Support but the uploaded information will not be associated with your My Oracle Support account. Therefore, if you log in to My Oracle Support with your credentials, you will not see this information displayed against your account. However, if you had specified an e-mail address, then you will continue to receive security updates and other notifications from Oracle to that e-mail address.
 - b. If the hosts where the Web tier and application tier are being provisioned have an *indirect* connection to the Internet through a proxy server, then specify an e-mail address and My Oracle Support password, and then in the Connection Details section, specify the proxy server details.

Note: You can change the proxy server settings any time after the Deployment Procedure ends. To do so, run the `configCCR` command from the `/ccr/bin/` directory within the Oracle home directory of the provisioned application server.

- c. If the hosts where the Web tier and application tier are being provisioned do not have a *direct* or *indirect* connection to the Internet, then specify the e-mail address and leave the other fields blank.

In this case, after you complete the installation process, manually collect the configuration information and upload it to My Oracle Support.

- d. Click **Next**.
9. On the Review page, review the details you have provided for provisioning a Web tier and application tier, and click **Submit**.

22.3.2.4 Provisioning and Treating Oracle Application Server as a Standalone Instance With Internet Directory

This section describes how you can provision the application tier and Web tier of Oracle Application Server 10g Release 1 (10.1.3), which are identical to the ones available on a gold image available in the Software Library, and treat that as a standalone instance with Internet directory.

In particular, this section covers the following:

- [Prerequisites](#)
- [Provisioning Procedure](#)

22.3.2.4.1 Prerequisites

Before running the Deployment Procedure, meet the following prerequisites:

Prerequisites for Designers

- Ensure that you meet the prerequisites described in [Chapter 2](#).
- Compare the configuration of the source and target hosts and ensure that they have the same configuration. If the configurations are different, then contact your system administrator and fix the inconsistencies before running the Deployment Procedure.

To compare the configuration of the hosts, in Cloud Control, click **Targets** and then **Hosts**. On the Hosts page, click the name of the source host to access its Home page, and then click the Configuration tab. On the Configuration page, click **Compare Configuration** and select the target host.

- If you are deploying multiple Web tiers, then ensure that a Software Load Balancer is set up and is accessible from the Web tier's hosts.

The Software Library provides a script to configure the F5 Big IP Application Switch (Software Version 4.5 PTF.5) load balancer on the selected Web tiers. For other systems such as Cisco CSM 3.1, overwrite the script with your specific configuration. The script is available in the following location of the Software Library:

```
Directives/Oracle Directives/Loadbalancer
```

- Ensure that the installation base directory, where the Web tier and application tier will be installed, is accessible (but not shared) on all target hosts.

Prerequisites for Operators

- If you have PAM/LDAP enabled in your environment, then ensure that the target agents are configured with PAM/LDAP. For more information, see My Oracle Support note 422073.1.
- Ensure that you use an operating system user that has the privileges to run the Deployment Procedure, and that can switch to *root* user and run all commands on the target hosts. For example, commands such as `mkdir`, `ls`, and so on.

If you do not have the privileges to do so, that is, if you are using a locked account, then request your administrator (a designer) to either customize the Deployment Procedure to run it as another user or ignore the steps that require special privileges.

For example, user account A might have the root privileges, but you might use user account B to run the Deployment Procedure. In this case, you can switch from user account B to A by customizing the Deployment Procedure.

For information about customization, see [Chapter 33](#).

22.3.2.4.2 Provisioning Procedure

To provision a Web tier and an application tier, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Middleware Provisioning**.
2. In the Deployment Procedures section, click **Application Server Provisioning Procedures**.
3. On the Deployment Procedure Manager page, in the Procedures subtab, from the table, select **Application Server Deployment 10.1.3**. Then click **Schedule Deployment**.
4. On the Source Selection page, in the Source Selection section, in the Select the Gold Image of an Oracle Home from the Software Library subsection, do the following:
 - a. Select **Select from Software Library**.
 - b. In the **Source for Web Tier** section, click the torch icon and select the generic component that contains the Web tier.
 - c. In the **Source for App Tier** section, click the torch icon and select the generic component that contains the application tier.

Note: When you click the torch icon to search for components, the Select Component page displays the components available in the Software Library. If you want to deploy a gold image, then select the gold image component that is either in **Ready** or **Active** status.

- d. Click **Next**.
5. On the Target List page, do the following:
 - a. In the Web Tier Hosts section, click **Add** to add hosts on which you want to deploy the Web tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the application tier.

- b. In the Application Tier Hosts section, click **Add** to add hosts on which you want to deploy the application tier. Ensure that the platform of this host is the same as the platform of the host on which you want to deploy the Web tier.
 - c. Click **Next**.
6. On the Credentials/Schedule page, do the following:

- a. In the Target Host Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- b. In the Agent Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

Note: You can optionally override these preferred credentials. The credentials you specify here are used by the Deployment Procedure to run the provisioning operation. If this environment is secure and has locked accounts, then make sure that:

- The credentials you specify here have the necessary privileges to switch to the locked account for performing the provisioning operation.
- The Deployment Procedures has been customized to support locked environments.

For more information, see [Chapter 33](#).

From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- c. In the Source Oracle Home Credentials section, retain the default section, that is, **Preferred Credentials** so that the preferred credentials stored in the Management Repository can be used.

To override the preferred credentials with another set of credentials, select **Override Preferred Credentials**. From the **Host Credentials** list, select **Same for all Oracle Homes** if you want to use the same operating system credentials across hosts, or select **Different for each Oracle Home** if you want to use different credentials for each host. According to the selection you make, specify the credentials. Ensure that the users belong to the same operating system group.

- d. In the Schedule section, schedule the Deployment Procedure to run either immediately or later.
- e. Click **Next**.

7. On the Application and Web Tier page, do the following:

- a. In the Cluster Details section, select **Standalone As**.
- b. In the Instance Details section, specify unique instance names for the Web tier instance and application tier instance, and specify the OC4J administrator password for the source host and the target host.

You can always change the default instance names with any other custom names. However, ensure that the names you specify are unique because, by default, the host name and domain name of that host are appended to the instance name you specify here.

IMPORTANT:

- Each Oracle Application Server 10g instance has its own password, regardless of which user performed the installation. Passwords are not shared across instances, even if the instances were installed by the same user.
- If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in the Additional Parameters section. For more information, see Step 7 (e).
- The passwords you specify here must contain a minimum of 5 and a maximum of 30 alphanumeric characters. It can include underscore (`_`), dollar (`$`), or pound (`#`) characters. It must start with an alphabet and must contain at least one numeric value.

-
-
- c. In the Port Details section, specify the HTTP load balancer host and listener ports to manage HTTP connections made by client applications. Alternatively, you can retain the default value, that is, `7777`. Select **Enable SSL** if you want to secure the communications.
 - d. In the Load Balancer Details section, select **Configure Load Balancer** and provide the required information if you have an F5 BIG-IP Local Traffic Manager load balancer configured.

NOTE: Cloud Control supports only F5 BIG-IP Local Traffic Manager. If you have any other load balancer, then deselect **Configure Load Balancer**, and manually configure that load balancer and the HTTP servers associated with it. Do not use this section in this case.

- e. In the Additional Parameters section, specify any additional Web tier-specific or application tier-specific parameters you want to pass to the Deployment Procedure. For example, `-debug`. You can specify any other Oracle Universal Installer (OUI) parameter that can be in this provisioning operation.

IMPORTANT: If you are cloning an application server with multiple OC4J instances that have different passwords, then ensure that you use the `-force` command as an additional parameter in this section.

This is to ensure that the password you specify in the Instance Details section is uniformly propagated to all OC4J instances that are being provisioned.

However, if you still want to maintain different passwords for the provisioned OC4J instances, then after the deployment procedure ends successfully, access the application server console and change the passwords for the individual OC4J instances.

- f. In the Identify Management Configuration section, select **Configure Java Authentication and Authorization Service (JAZN) with a LDAP-based provider**.

Using this option, you can set up JAZN LDAP-based provider for authentication and authorization for OC4J application.

Java Authentication and Authorization Service (JAAS) is a Java package that enables services and applications to authenticate and enforce access controls upon users. Oracle Application Server 10g Containers for J2EE (OC4J) supports JAAS by implementing a JAAS provider (also called as JAZN).

The JAAS provider provides application developers with user authentication, authorization, and delegation services to integrate into their application environments. It also supports JAAS policies. Policies contain the rules (permissions) that authorize a user to use resources, such as reading a file and so on.

- g. Click **Next**.
8. On the Identity Management page, do the following:
 - a. In the Identity Management Host Details section, specify the connection information for the Internet Directory to be used for Identity Management of the Oracle Application Server users and groups. If you do not have an Internet Directory installed, install it using the OracleAS Infrastructure component.
 - b. In the Internet Directory Login Details section, specify credentials of the user who belongs to the iASAdmin group in the Internet Directory.
 - c. Click **Next**. Cloud Control displays the Configure Oracle Home page.
9. On the Configure Oracle Home page, do the following:
 - a. If the hosts where the Web tier and application tier are being provisioned have a *direct* connection to the Internet, then specify an e-mail address and My Oracle Support password.

An e-mail address is required so that security updates and install updates can be sent. You can specify any e-mail address, but Oracle recommends you to specify the My Oracle Support user name. For example,
`john.mathew@xyz.com`.

If the My Oracle Support password is incorrect, you will be allowed two more attempts. However, if your password is incorrect in all three attempts or if it is left blank, then you are registered anonymously, which means, the configuration information will be collected and uploaded to My Oracle Support but the uploaded information will not be associated with your My

Oracle Support account. Therefore, if you log in to My Oracle Support with your credentials, you will not see this information displayed against your account. However, if you had specified an e-mail address, then you will continue to receive security updates and other notifications from Oracle to that e-mail address.

- b. If the hosts where the Web tier and application tier are being provisioned have an *indirect* connection to the Internet through a proxy server, then specify an e-mail address and My Oracle Support password, and then in the Connection Details section, specify the proxy server details.

Note: You can change the proxy server settings any time after the Deployment Procedure ends. To do so, run the `configCCR` command from the `/ccr/bin/` directory within the Oracle home directory of the provisioned application server.

- c. If the hosts where the Web tier and application tier are being provisioned do not have a *direct* or *indirect* connection to the Internet, then specify the e-mail address and leave the other fields blank.

In this case, after you complete the installation process, manually collect the configuration information and upload it to My Oracle Support.

- d. Click **Next**.

10. On the Review page, review the details you have provided for provisioning a Web tier and application tier, and click **Submit**.

22.4 Provisioning Oracle SOA Suite 10g (10.1.3.4 and 10.1.3.5)

The use cases and the prerequisites and deployment instructions for each of the use cases for provisioning Oracle SOA Suite 10g (10.1.3.4 and 10.1.3.5) are almost the same as the ones described in [Section 22.3](#).

The only difference is that in Step (3), on the Deployment Procedure Manager page, in the Procedures tab, from the table, you must select **Application Server Deployment 10.1.3.xSOA**, then select **Schedule Deployment**.

Part VI

Bare Metal Server Provisioning

This part contains the following chapter:

- [Chapter 23, "Provisioning Bare Metal Servers"](#)

Provisioning Bare Metal Servers

This chapter explains how you can provision Linux on bare metal servers using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following. In particular, this chapter contains the following sections:

- [Getting Started with Provisioning Bare Metal Servers](#)
- [Understanding Bare Metal Provisioning](#)
- [Supported Releases of Linux](#)
- [Setting Up Infrastructure for Bare Metal Provisioning](#)
- [Provisioning Bare Metal Servers](#)

Tip: Before you begin provisioning of Linux on bare metal boxes, it is advisable to set preferred credentials for the Stage Server. If not, follow instructions in [Section 2.3.4](#) to set up preferred credentials. If you want to use a reference host, set credentials for the reference host also. You can also set preferred credentials when configuring the deployment procedure for provisioning Linux.

Note: Before starting the provisioning Linux operations, ensure that you configure sudo privileges. For more information about configuring sudo privileges, see [Section 2.3.3](#).

23.1 Getting Started with Provisioning Bare Metal Servers

This section helps you get started with this chapter by providing an overview of the steps involved in provisioning Linux operating system. Consider this section to be a documentation map to understand the sequence of actions you must perform to successfully provision Linux operating system. Click the reference links provided against the steps to reach the relevant sections that provide more information.

Table 23-1 *Getting Started with Provisioning Linux Operating System*

Step	Description	Reference Links
Step 1	<p>Knowing About The Supported Releases</p> <p>Know what releases of Linux are supported for provisioning.</p>	To learn about the releases supported for Linux Provisioning, see Section 23.3 .

Table 23–1 (Cont.) Getting Started with Provisioning Linux Operating System

Step	Description	Reference Links
Step 2	<p>Knowing the Use Case</p> <p>This chapter covers provisioning Linux. Understand the use case for Linux provisioning.</p>	<ul style="list-style-type: none"> To learn about provisioning bare metal boxes, see Section 23.5.
Step 3	<p>Setting Up Infrastructure</p> <p>Before you perform Linux provisioning, you must meet the prerequisites, such as setting up of the provisioning environment, applying mandatory patches, setting up of Oracle Software Library.</p>	<ul style="list-style-type: none"> To learn about the prerequisites to be met for provisioning bare metal boxes, see Section 23.4.
Step 4	<p>Provisioning Linux</p> <p>Provision Linux on bare metal boxes.</p>	<ul style="list-style-type: none"> To provision Linux on bare metal boxes, follow the steps explained in Section 23.5.2.

23.2 Understanding Bare Metal Provisioning

Proliferation of low cost servers in our data centers has brought in a fresh set of management challenges. The well-acknowledged problems include the difficulty in managing consistency and compatibility across operating system and software deployments, server drifts and security vulnerabilities that lead to lack of compliance, difficulty in deploying software, difficulty in provisioning new servers with variety of configurations and applications, high cost of operation and difficulty in adapting to changes in workload of the environment. These lead to system administrators and DBAs spending significant amount of their time in software and server provisioning operations.

Oracle's answer to the Software and Server Management challenge is its Bare Metal Provisioning Application, which is a part of Cloud Control Lifecycle Management Pack available at <http://www.oracle.com/technetwork/oem/lifecycle-mgmt-495331.html> Bare Metal Provisioning Application addresses the data center, server farm challenge to provision software and servers quickly, efficiently, and make them operational.

The application uses standardized PXE (Pre Boot Execution environment) booting process for provisioning both bare-metal and live servers. It provides a role based User Interface, for easily creating gold images and initiating automated, unattended installs.

23.2.1 Overview of the Bare Metal Provisioning Environment

The deployment environment in the data center needs to be setup in a certain manner in order to support the provisioning application. Besides the Oracle Management Server (OMS) which hosts Cloud Control and Provisioning Application, the following need to be setup and configured before using the provisioning application.

Software Library and its Entities

For information about configuring Software Library and its entities, see [Section 2.2](#).

Boot Server

One of the key requirements of application is the ability of the hardware server to boot up over the network (rather than from a local boot device). A boot server must be set

up so that it is able to service the requests from the designated hardware servers in order for them to boot over the network. Boot server must be an Cloud Control target and should be able to receive the BOOTP and TFTP (Trivial File Transfer Protocol) requests over the network from the hardware server. Refer to [Section 23.4.2](#) for setting up a boot server with DHCP/TFTP combination. Also refer to section [Section 23.4.5](#). It is also recommended that the users read about DHCP, PXE, and Redhat Kickstart technology before going through the boot server setup. Refer to [Appendix D](#) for a detailed discussion on PXE.

Stage Server

During provisioning of an image on hardware servers, the required binaries and files are first transferred to a stage server. This is known as **Staging** phase and is responsible for preparing images to be installed over the network, and exposing installable or executable software elements over the network to the target hardware server being provisioned.

The Provisioning application requires at least one stage server on which all the activities related to staging can be performed. Stage server should again be an Cloud Control target. Refer to section [Section 23.4.1](#) for setting up a stage server. Also refer to section [Section 23.4.4](#).

Reference Host

A Reference Host (also called a **gold machine**) is the machine that the Provisioning application uses as a reference to create the Linux operating system component. The Provisioning application picks up the list of RPMs (along with their versions) installed on the reference host, and fetches those RPMs from a RPM repository to create an Linux OS component that represents the operating system installed on the reference host. The reference host must be an Cloud Control target.

RPM Repository

The Provisioning application picks up the RPMs for the operating system from the RPM repository. At least one repository needs to be setup for use by the Provisioning application. From the networking perspective, you are advised to keep the RPM Repository as close to the target machines as possible. It will help in bringing down the installation time drastically by reducing the time taken to transfer RPMs from the RPM Repository to the hardware servers. If you have multiple hardware server groups residing at physically different locations, it would be better to have one RPM Repository for each of these locations. Refer to section [Section 23.4.3](#) for setting up a RPM repository. Also refer to section [Section 23.4.7](#).

23.2.2 Overview of the Bare Metal Provisioning Process

The provisioning process consists of the following two high-level tasks:

1. Setting Up Provisioning Environment ([Section 23.4](#)):
 - Setting up and configuring Boot/DHCP server and Stage server, setting up RPM repository and Software Library
 - Optionally, creating baremetal provisioning entities
2. Provisioning Linux using Bare Metal Provisioning Application ([Section 23.5](#)):
 - Launching the Baremetal Provisioning wizard to configure the bare metal machines using MAC addresses, subnet, or re-imaging Cloud Control hosts.

- Powering up the bare metal machine on the network to begin the PXE-based OS boot and install process. For information about PXE Booting and KickStart, see [Appendix D](#).

23.3 Supported Releases of Linux

Cloud Control supports bare metal provisioning of 32-bit and 64-bit variants of the following operating systems:

- Oracle Linux 5.0 or higher
- Oracle Linux 4.0 or higher
- RedHat Enterprise Linux (RHEL) 5.0 or higher
- RedHat Enterprise Linux (RHEL) 4.0 update 2 or higher
- RedHat Enterprise Linux (RHEL) 3.0 update 6 or higher
- SuSE Linux (SLES) 10

23.4 Setting Up Infrastructure for Bare Metal Provisioning

This section describes how to set up the infrastructure required to provision bare metal machine. In particular, this section describes the following:

23.4.1 Setting Up Stage Server

Stage server must meet the following requirement:

- **NFS or HTTP Support**

During the installation, hardware servers mount the stage directory so that all the files required for installation appear as local files. In such a scenario, the stage server functions as the NFS server and the hardware servers as its clients. If the stage server uses NAS for staging storage, the NAS server should have the NFS support.

If the stage server cannot have NFS support, it must be accessible by HTTP.

Follow the instructions listed below to set up a Linux machine as the stage server:

1. Create a top-level directory on the stage server where all the files will be stored. In the following steps, **STAGE_TOP_LEVEL_DIRECTORY** refers to the absolute path of this top-level directory.

You can specify the HTTP or NFS location of agent rpms when you set up a default image in the Provisioning application. Alternatively, you can copy agent rpms to **STAGE_TOP_LEVEL_DIRECTORY** so that they are picked up automatically.

To get and copy agent RPMs to **STAGE_TOP_LEVEL_DIRECTORY**, run the following EMCLI command:

```
emcli get_agentimage_rpm -destination=<STAGE_TOP_LEVEL_DIRECTORY>  
-platform="Linux x86_64"
```

2. Configure NFS services. Perform the following steps on the stage server.

Note: If the stage server uses **NAS** for staging storage, the following steps need to be performed on the **NAS server** as well.

- a. Ensure the NFS service is running. One can check this by running **service nfs status**.

Modify the `/etc/exports` file to have the following entry:

```
{Directory path} {host_name_or_ip_prefix}* (ro,sync)
```

For example, `/STAGE_TOP_LEVEL_DIRECTORY 10.152.* (ro,sync)`, if the hardware servers to be provisioned have the IP prefix 10.152.

Or, `/STAGE_TOP_LEVEL_DIRECTORY provision-host* (ro,sync)`, if the hardware servers to be provisioned have names starting with `provision-host`.

- b. After the modification is made, run the **service nfs restart** command to make the changes visible to nfs daemons.
- c. Install a Management Agent.

Refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide* to install a 12.1.0.1.0 or higher version of Management agent on the Stage Server.

Note: Ensure that the preferred credentials set for the staging server host has "write" access to the staging storage.

- d. From Cloud Control console, set the privileged preferred credentials and sudo privilege for the stage server.

Oracle recommends that the stage server must have very limited access due to the criticality and sensitivity of the data it hosts. The super administrator can enforce this by creating one account on the stage server, and setting it as the preferred credential, to be used by all the provisioning users in Cloud Control. This preferred credential should also be a valid ORACLE_HOME credential (belonging to ORACLE_HOME owner's group).

23.4.2 Setting Up Boot Server and DHCP Server

Note: Ensure that you have 2 GB RAM available for boot server, stage server, and RPM repository server.

If you have the required boot server, stage server, and RPM repository already created, then set up the preferred credentials.

Complete the following steps to setup a machine as the boot server:

1. Install DHCP and TFTP Servers if not already installed.

The two servers could be running either on the same machine, or on different machines. Oracle recommends running the TFTP server on the same host machine as the DHCP server. In case the two servers are installed and configured on different machines, the machine running the TFTP server will be referred to as the boot server.

2. Configure the TFTP server:

- Ensure that the pxelinux boot loader (**pxelinux.0**) exists in the directory that is configured for your TFTP server (`/tftpboot/linux-install` in the given examples).

3. Configure DHCP Server:

Edit the **dhcpd.conf** (*/etc/dhcpd.conf*) file. A sample **dhcpd.conf** file for PXE setup is shown below:

```
allow booting;
allow bootp;

option domain-name <domain_name>;
option domain-name-servers dns_servers;
option routers <default_router>;

subnet <subnet-number> netmask <netmask> {
    [ parameters ]
    [ declarations ]
}
# Group the PXE bootable hosts together

group {

# PXE-specific configuration directives...

    next-server <TFTP_server_IP_address>;

    filename "linux-install/pxelinux.0";

    host <hostname> {
        hardware ethernet <MAC address>;
        fixed-address <IP address>;
    }
}
```

The *next-server* option in the DHCP configuration file specifies the host name or IP Address of the machine hosting the TFTP server. Oracle recommends running the TFTP Server on the same host machine as the DHCP Server. Therefore, this address should be the IP Address or host name for the local machine.

The *filename* option specifies the boot loader location on the TFTP server. The location of the file is relative to the main TFTP directory.

Any standard DHCP configuration file is supported. The sample file format above shows one entry (line 12-15) for each target host. The DHCP service must be restarted every time you modify the configuration file.

4. Enable the tftp service. Edit the */etc/xinetd.d/tftp* file to change the disable flag as no (default=no).

5. Restart the following services:

```
service dhcpd restart
service xinetd restart
service portmap restart
```

6. Install Oracle Management Agent. This step is not necessary if the DHCP and Boot servers are installed on the Cloud Control server.

Note: Refer to *Oracle Enterprise Manager Cloud Control Basic Installation Guide* to install a 12.1.0.1.0 or higher version of Management agent on the boot server.

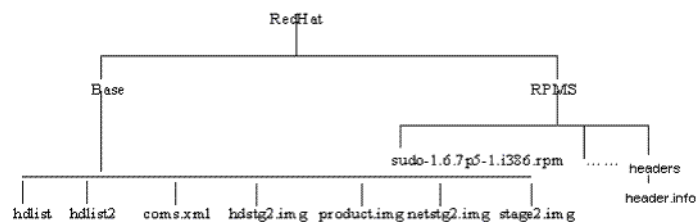
23.4.3 Setting Up RPM Repository

Note: It is recommended that you use RAM of 2 GB.

23.4.3.1 Setting UP RHEL 4 RPM Repository

RPM Repository is used as the source of Linux and application packages that need to be installed on the newly provisioned bare metal box. For example, an RPM Repository may be created to contain all the 32-bit Linux rpms and another repository may be created to contain Linux x86-64 bit rpms. Two separate Linux images can then be created each based on one of the repositories.

RHEL RPM repository to be used should have the following Red Hat Install tree structure:



There are multiple ways to create a RPM repository. If Red Hat Enterprise Linux CDs are available, do the following:

1. Copy all the contents of the first CD to a directory say RPM_REPOS.
2. Copy all rpms from other CDs to <RPM_REPOS>/Redhat/RPMS. Change directory to the RPMS directory:


```
cd <RPM_REPOS>/Redhat/RPMS
```
3. Add custom RPMs to the repository as follows:
 - a. If there are custom RPMs installed on the reference host that need to be provisioned on the bare metal machine, make sure to copy them to the following repository location:


```
<RPM_REPOS>/Redhat/RPMS
```
 - b. Install anaconda-runtime RPM on the machine hosting the RPM repository. This might require other dependent packages to be installed.
 - c. Run the following commands:


```
cd /usr/lib/anaconda-runtime
./genhdlist --productpath=RedHat --withnumbers --hdlist <RPM_REPOS>/RedHat/base/hdlist <RPM_REPOS>
```
4. Run yum-arch :

This should create a **headers** directory. Make sure this directory contains a **header.info** file.

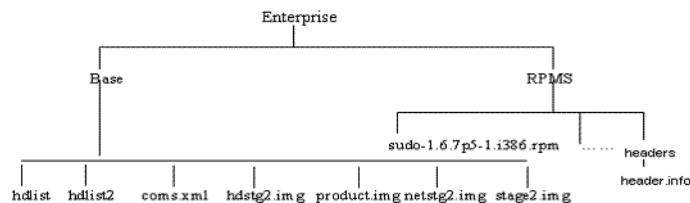
If yum is not installed then download it from the Linux Vendor's Web site.
5. Create a symbolic link in /var/www/html to <RPM_REPOS> directory.

The repository should now be available through HTTP if an Apache server is running.

Note: If the Apache server that comes with Enterprise Manger Cloud Control is used, enable the Apache directory index page using the "Options Indexes" directive in the Apache configuration (httpd.conf) file.

23.4.3.2 Setting Up Oracle Linux 4 RPM Repository

Oracle Linux RPM repository should have the Install tree structure shown below:



You can set up Oracle Linux Repository by using the Oracle Linux installation media as follows:

1. Download Oracle Linux from <http://edelivery.oracle.com/linux>.
2. Copy all the contents of the first CD to a directory say **RPM_REPOS**.
3. Copy all rpms from other CDs to <RPM_REPOS>/Enterprise/RPMS. Change directory to the RPMS directory:

```
cd <RPM_REPOS>/Enterprise /RPMS
```

4. Add custom RPMs to the repository.
 - a. If there are custom RPMs installed on the reference host that need to be provisioned on the bare metal machine, make sure to copy them to the following repository location:

```
<RPM_REPOS>/Enterprise/RPMS
```

- b. Install anaconda-runtime RPM on the machine hosting the RPM repository. This might require other dependent packages to be installed.

- c. Run the following commands:

```
cd /usr/lib/anaconda-runtime
./genhdlist --productpath=Enterprise --withnumbers --hdlist <RPM_REPOS>/Enterprise/base/hdlist <RPM_REPOS>
```

5. Run `yum-arch` :

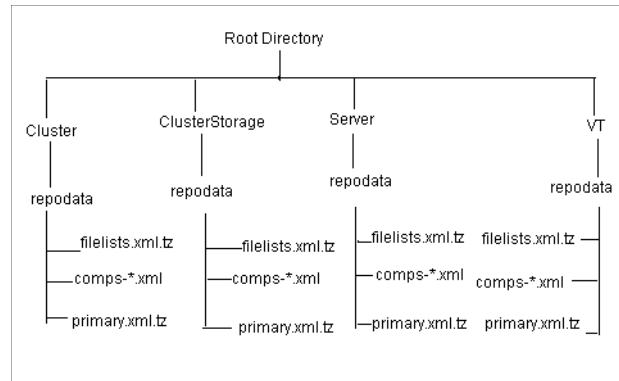
This should create a **headers** directory. Make sure this directory contains a **header.info** file.

6. Create a symbolic link in `/var/www/html` to <RPM_REPOS> directory.

The repository should now be available through HTTP if an Apache server is running.

23.4.3.3 Setting Up RHEL 5/Oracle Linux 5 RPM Repository

Oracle Linux RPM repository should have the Install tree structure shown below:



You can set up Oracle Linux Repository by using the Oracle Linux installation media as follows:

1. Download Oracle Linux from <http://edelivery.oracle.com/linux>.
2. Copy all the contents of the first CD to a directory say Root Directory.
3. Copy all contents from the Cluster, ClusterStorage, Server, and VT directories in the other CD to the respective directories.
4. Run createrepo for all four directories. For example:

```
createrepo <Root Directory>/cluster
```

5. Add custom RPMs to the repository as follows:
 - a. If there are custom RPMs installed on the reference host that need to be provisioned on the bare metal machine, make sure to copy them to the directory containing the RPMs, such as Cluster, VT, ClusterStorage, and Server.
 - b. Run the createrepo command on this directory. For example:

```
createrepo ClusterStorage
```

6. Create a symbolic link in /var/www/html to <Root Directory> directory.

The repository should now be available through HTTP if an Apache server is running.

23.4.3.4 Exposing RPM Repository through HTTP or FTP

To expose RPM Repository through HTTP, follow these steps:

1. Ensure that Apache Web Server is installed and HTTP service is running.
2. Create a symbolic link in document root to RPM Repository directory. For example, /var/www/html to <RPM_REPOS> directory.

To expose RPM Repository through FTP, ensure that FTP server is running.

23.4.4 Configuring Stage Server

During provisioning of an image on hardware servers, the required binaries and files are first transferred to a stage server. This is known as Staging phase and is responsible for preparing images to be installed over the network, and exposing installable or executable software elements over the network to the target hardware server being provisioned.

The Provisioning application requires at least one stage server on which all the activities related to staging can be performed. From the networking perspective, you are advised to keep the stage server as close to the target machines as possible. It will help in bringing down the installation time drastically, by reducing the time taken to transfer image data from the stage server to the hardware servers. If you have multiple hardware server groups residing at physically different locations, it would be better to have one stage server for each of these locations. Stage server should again be an Cloud Control target.

Follow these steps:

1. Log in to Cloud Control as an administrator.
2. From the **Enterprise** menu, select **Provisioning and Patching** and then select **Bare Metal Provisioning**.
3. In the Infrastructure tab, in the Stage Servers section, click **Add Server**.
4. In the Add Staging Server dialog, select a **Stage Server**, specify a **Stage Directory**, for example, `/scratch/stage`, and **Base URL**, for example, `file://stgserver.example.com/scratch/stage`. Click **OK**.

Exporting Stage Directory on the Stage Server

1. Run the following commands:

```
$ su - root
# mkdir /scratch/stage
# vi /etc/exports
```

2. Add the following:

```
/scratch/stage *(ro, sync)
# service nfs restart
# exportfs (verify)
```

23.4.5 Configuring Boot Server

One of the key requirements of application is the ability of the hardware server to boot up over the network (rather than from a local boot device). A boot server must be set up so that it is able to service the requests from the designated hardware servers in order for them to boot over the network. Boot server must be an Cloud Control target and should be able to receive the BOOTP and TFTP (Trivial File Transfer Protocol) requests over the network from the hardware server. Refer to Setting Up Boot Server for setting up a boot server with DHCP/TFTP combination.

Follow these steps:

1. Read about DHCP, PXE, and Redhat Kickstart technology before going through the boot server setup.
2. Ensure that you have administrator privileges.
3. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Bare Metal Provisioning**.
4. In the Infrastructure tab, in the Boot Servers section, click **Add**.
5. In the Add Boot Server dialog, select a **Boot Server** and specify a **TFTP Boot Directory**, for example, `/tftpboot/linux-install/`. Click **OK**.

23.4.6 Configuring DHCP Server

Follow these steps:

1. Ensure that you have administrator privileges.
2. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Bare Metal Provisioning**.
3. In the Infrastructure tab, in the DHCP Servers section, click **Add**.
4. In the Add DHCP Server dialog, select a **DHCP Server** and specify a **DHCP Configuration File**, for example, `/etc/dhcpd.conf` that has been modified to support your target hosts. Click **OK**.

23.4.7 Configuring RPM Repository

The Provisioning application picks up the RPMs for the operating system from the RPM repository. At least one repository needs to be setup for use by the Provisioning application.

Follow these steps:

1. Ensure that you have administrator privileges.
2. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Bare Metal Provisioning**.
3. In the Infrastructure tab, in the RPM Repositories section, click **Add**.
4. In the Add RPM Repository Server dialog, specify a **Repository Name** and **URL**. For RPM repository either accessible by HTTP or on a local server, specify the URL in the HTTP format, for example, `http://example.com/OEL5/`. For NFS location, specify the URL as `file://example/OEL5/`.

Click **OK**.

23.4.8 Checklist for Boot Server, Stage Server, RPM Repository, and Reference Host

Ensure that the following criteria are met before provisioning:

Table 23–2 Checklist for Boot Server, Stage Server, RPM Repository, and Reference Host

Resource Name	Checklist
Boot Server	<p>DHCP server is up and running.</p> <p>The <code>next_server</code> entry in <code>/etc/dhcpd.conf</code> file points to this boot server.</p> <p>TFTP is up and running.</p> <p>Boot Server is present in the same subnet where the target machines to be provisioned are present or will be added.</p> <p>Management Agent is installed.</p> <p>Boot server machine is visible as a managed target in Cloud Control.</p> <p>A brand new PXE-bootable box actually detects the boot server and starts to boot it (even if no image is installed yet)</p>

Table 23–2 (Cont.) Checklist for Boot Server, Stage Server, RPM Repository, and Reference Host

Resource Name	Checklist
Stage Server	<p>Large storage, High Memory and Sufficient Memory.</p> <p>If NAS server is used for storage then it should have NFS support.</p> <p>Management Agent is installed.</p> <p>Boot server machine is visible as a managed target in Cloud Control.</p> <p>The required agent rpm is staged for installing agents on targets.</p> <p>Preferred Credentials are set.</p> <p>Stage server is reachable from the box to be provisioned (or the same subnet)</p>
RPM Repository	<p>RPM Repository is as close as possible to the target servers.</p> <p>Install tree structure is as indicated in Configure RPM repository section.</p> <p>RPM repository is available via HTTP.</p> <p>Provide the exact URL and test the RPM repository access over HTTP</p>
Reference Host	<p>Agent is installed on local disk and not on NFS mounted directory.</p> <p>Preferred Credentials are set.</p>
Software Library	<p>Shared storage used for Software Library is accessible through NFS mount points to all OMS servers.</p>

23.4.9 Configuring Software Library

To set up and configure the Software Library, see [Section 2.2](#).

You can create the following Bare Metal provisioning entities and store them in Software Library:

- [Creating Operating System Component](#)
- [Creating Disk Layout Component](#)

23.4.9.1 Creating Operating System Component

Follow these steps to create an operating system component:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. From the Software Library Home, from the **Actions** menu, select **Create Folder**.
3. In the Create Folder popup, specify a **Name** and **Description** for the folder and select the folder location. For example, create a folder `BMP-OEL56` to represent the components you will use to provision a bare metal server of Oracle Linux v5.6. Click **Save**.
4. From the **Actions** menu, select **Create Entity** and then **Bare Metal Provisioning Components**.
5. In the Create Entity: Bare Metal Provisioning Components dialog box, select **Operating System Component** and click **Continue**.

6. On the Describe page, enter the **Name**, **Description**, and **Other Attributes** that describe the entity.

Note: The component name must be unique to the parent folder that it resides in. Sometime even when you enter a unique name, it may report a conflict, this is because there could be an entity with the same name in the folder that is not visible to you, as you do not have view privilege on it.

Click **+Add** to attach files that describe the entity better like readme, collateral, licensing, and so on. Ensure that the file size is less than 2 MB.

In the **Notes** field, include information related to the entity like changes being made to the entity or modification history that you want to track.

7. In the Basic Operating System page, select a **Time Zone** and specify the **Root Password**.

In the Operating System Users List, add the users for the operating system by specifying the **User Name**, **Password**, **Primary Group**, and **Additional Groups**. Specify if you want to **Enable Sudo Access** for the user.

In the Fetch Configuration properties from Reference Enterprise Manager Host target section, select **Fetch Properties** to apply the host properties. Select the reference host and select the **Configurations** you want to fetch.

Click **Next**.

8. In the Advanced Configuration page, specify the agent properties, boot configuration, and other configuration as explained in the tables.

The Configure Package Selection section displays the packages from the operating component or reference host you specified in the previous screen. You can retain or remove these packages from the component.

Click **Next**.

9. In the Review page, verify the information and click **Finish**.

The operating system component will be saved in Software Library with the status Ready.

Table 23–3 Agent Settings

Element	Description
Install User	User name for installing the agent.
Install Group	Install group for agent.
Agent Registration Password	Specify the password to be used to register the agent with Oracle Management Server.
RPM URL	Location where agent RPMs are stored.

Table 23–4 Additional OS Configuration

Element	Description
Require TTY	Select this option if you want sudo user to Log in to a separate terminal.
SELinux	You can choose to enable or disable SELinux.

Table 23–4 (Cont.) Additional OS Configuration

Element	Description
Mount Point Settings	Specify entries for the <code>/etc/fstab</code> file. You can specify mount points on the newly provisioned Linux machine. By default, mount point settings from the reference Linux machine are inherited.
NIS Settings	Specify entries for the <code>/etc/yp.conf</code> file. You can specify NIS settings for the newly provisioned Linux machine. By default, NIS settings from the reference Linux machine are inherited.
NTP Settings	Specify entries for the <code>/etc/ntp.conf</code> file. You can specify NTP settings for the newly provisioned Linux machine. By default, NTP settings from the reference Linux machine are inherited.
Kernel Parameter Settings	Specify scripts for Kernel Parameters.
Initab Settings	Specify settings for <code>/etc/inittab</code> file. All processes are started as part of init operation in boot process. Init operation decides the processes that will start on booting of a machine or when runlevel changes.
Firewall Settings	Specify firewall settings for the Linux target. Firewall settings are disabled by default and can be configured. Make sure that the port used by Management Agent is open for its communication with the Management Service. By default, Management Agent uses port 3872 or a port number in the range 1830-1849, unless configured to use some other port.

Table 23–5 Boot Configuration and Configuration Scripts

Element	Description
Advanced Configuration & Power Interface	Specify settings for boot time parameter for kernel (acpi) in the <code>/boot/grub/grub.conf</code> file.
Use Para-Virtualized kernel	Select if you are using para-virtualized kernel.
Post Install Script	Specify any set of commands that need to be executed on the newly provisioned machine. These commands will be appended to the post section of the kickstart file.
First Boot Script	Specify any set of commands that need to be executed on the newly provisioned machine when it starts up for the first time.

23.4.9.2 Creating Disk Layout Component

Follow these steps to create a disk layout component:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. From the Software Library Home, from the **Actions** menu, select **Create Folder**.
3. In the Create Folder popup, specify a **Name** and **Description** for the folder and select the folder location. Click **Save**.
4. From the **Actions** menu, select **Create Entity** and then **Bare Metal Provisioning Components**.
5. In the Create Entity: Bare Metal Provisioning Components dialog box, select **Disk Layout Component** and click **Continue**.
6. On the Describe page, enter the **Name**, **Description**, and **Other Attributes** that describe the entity.

Note: The component name must be unique to the parent folder that it resides in. Sometime even when you enter a unique name, it may report a conflict, this is because there could be an entity with the same name in the folder that is not visible to you, as you do not have view privilege on it.

Click **+Add** to attach files that describe the entity better like readme, collateral, licensing, and so on. Ensure that the file size is less than 2 MB.

In the **Notes** field, include information related to the entity like changes being made to the entity or modification history that you want to track.

7. In the Configure page, specify the hard disk, RAID, partition, and logical configurations.

To specify the hard disk profile, click **Add**. Specify the **Mount Point**, **RAID Level**, **Partitions**, and **File System Type**.

To specify the Partition Configuration, click **Add**. Specify the **Mount Point**, **Device Name**, **File System Type**, and **Size (MB)**.

To specify RAID configuration, click **Add**. Specify the **Device Name** and **Capacity**.

To specify the Logical Volume Group Configuration, click **Add**. Specify the **Group Name**, **Partitions**, and **RAIDs**.

To specify the Logical Volume Configuration, click **Add**. Specify the **Mount Point**, **Logical Volume Name**, **Logical Group Name**, **File System Type**, and **Size (MB)**.

Click **Next**.

8. In the Review page, verify the information and click **Finish**.

The disk layout component will be saved in Software Library with the status Ready.

23.4.10 Creating an Oracle Virtual Server Component

Follow these steps to create an operating system component:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. From the Software Library Home, from the **Actions** menu, select **Create Folder**.
3. In the Create Folder popup, specify a **Name** and **Description** for the folder and select the folder location.
4. From the **Actions** menu, select **Create Entity** and then **Bare Metal Provisioning Components**.
5. In the Create Entity: Bare Metal Provisioning Components dialog box, select **Oracle Virtual Server Component** and click **Continue**.
6. On the Describe page, enter the **Name**, **Description**, and **Other Attributes** that describe the entity.

Note: The component name must be unique to the parent folder that it resides in. Sometime even when you enter a unique name, it may report a conflict, this is because there could be an entity with the same name in the folder that is not visible to you, as you do not have view privilege on it.

Click **+Add** to attach files that describe the entity better like readme, collateral, licensing, and so on. Ensure that the file size is less than 2 MB.

In the **Notes** field, include information related to the entity like changes being made to the entity or modification history that you want to track.

7. In the Basic Operating System page, select a **Time Zone** and specify the **Root Password** and the **OVM Agent Password**.

In the Operating System Users List, add the users for the operating system by specifying the **User Name**, **Password**, **Primary Group**, and **Additional Groups**. Specify if you want to **Enable Sudo Access** for the user.

Click **Next**.

8. In the Advanced Configuration page, specify the Dom0 Configuration, Boot Configurations, and Additional OS Details as explained in the tables.

Click **Next**.

9. In the Review page, verify the information and click **Finish**.

The oracle virtual server component will be saved in the Software Library with the status Ready.

Table 23–6 Additional OS Details

Element	Description
Mount Point Settings	Specify entries for the /etc/fstab file. You can specify mount points on the newly provisioned Linux machine. By default, mount point settings from the reference Linux machine are inherited.
NIS Settings	Specify entries for the /etc/yp.conf file. You can specify NIS settings for the newly provisioned Linux machine. By default, NIS settings from the reference Linux machine are inherited.
NTP Settings	Specify entries for the /etc/ntp.conf file. You can specify NTP settings for the newly provisioned Linux machine. By default, NTP settings from the reference Linux machine are inherited.
Kernel Parameter Settings	Specify scripts for Kernel Parameters.
Initab Settings	Specify settings for /etc/inittab file. All processes are started as part init operation in boot process. Init operation decides the processes that will start on booting of a machine or when runlevel changes.
Firewall Settings	Specify firewall settings for the Linux target. Firewall settings are disabled by default and can be configured. Make sure that the port used by Management Agent is open for its communication with the Management Service. By default, Management Agent uses port 3872 or a port number in the range 1830-1849, unless configured to use some other port.

Table 23–7 Boot Configuration and Configuration Scripts

Element	Description
Post Install Script	Specify any set of commands that need to be executed on the newly provisioned machine. These commands will be appended to the post section of the kickstart file.
First Boot Script	Specify any set of commands that need to be executed on the newly provisioned machine when it starts up for the first time.

23.5 Provisioning Bare Metal Servers

The following sections explain how to provision Linux on bare metal boxes:

- [Prerequisites](#)
- [Procedure](#)

Note: For information about downloading the Management Agent RPM kits, access the following URL:

http://www.oracle.com/technology/software/products/oem/htdocs/provisioning_agent.html

For instructions to install a Management Agent RPM kit, read the README file associated with the Management Agent RPM kit you are downloading.

23.5.1 Prerequisites

- Ensure that you meet the prerequisites described in [Setting Up Oracle Software Library](#).
- Ensure that you set up the bare metal provisioning infrastructure described in [Section 23.4](#).
- Ensure that you have Cloud Control administrator privileges.

23.5.2 Procedure

Follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Bare Metal Provisioning**.
2. In the Server Image section, from the **Provision** menu, select **Operating System**.
3. In the General/Target Selection page, in the General section, specify the **Deployment Name**. Select the **Operating System** you want to provision and provide a description. Select the **Patching Groups** and **Monitoring Templates** you want to associate with the system.

In the Target Selection section, select the Provisioning Category as one of the following:

- **MAC Addresses** if you want to provision the bare metal systems by specifying MAC addresses. Click **Add** to specify the list of MAC Address. In the Add MAC dialog box, specify the MAC addresses. Click **OK**.

Optionally, click **Add from File** to add the MAC address from a file. In the Add from File dialog box, click **Browse** and select the file from the location where you have stored it.

- **Subnet** to specify the subnet for the bare metal provisioning. In the Subnet to be Provisioned section, specify the **Subnet IP**, **Netmask**, **Number of Network Interfaces**, and **Bootable Network Interface**.
- **Re-image EM Host Targets** to re-provision an existing Cloud Control host target. In the Enterprise Manager Hosts to be Provisioned section, click **Add** to search and select the host target. Click **OK**. Select the **Bootable Network Interface**.

Optionally, you can click **Save As Plan** and save the configuration details you have specified. Specify a name and description and click **OK** to save the plan. You can later use the saved plan to provision bare metal boxes. You can save as plan on

any page of the wizard or configure the wizard completely and save the plan on the last page of the wizard.

Click **Next**.

4. In the Deployment page, in the Infrastructure section, specify:
 - a. **Stage Server** and select the **Storage**. Select **Run Stage Server Pre-requisite checks** to check if the stage server is configured properly.
 - b. **Boot Server** and select **Run Boot Server Pre-requisite checks** to check if the Boot server is configured properly.
 - c. **DHCP Server** and select **Run DHCP Server Pre-requisite checks** to check if the DHCP server is configured properly.
 - d. **Local RPM Repository**.

In the Fetch Configuration Properties from Pre-Created Components section, select the **Operating System Component**, **Disk Layout Component**, and **Provisioning Directive** from the Software Library. Otherwise, you can specify the operating system, disk layout, and other properties in the respective pages.

Click **Next**.

5. In the Basic OS Details page, set the **Time Zone** and **OS Root Password**. In the Add Operating System Users list section, click **Add**. Specify the **User Name**, **Password**, **Primary Group**, and **Additional Groups** to add the operating system users. Enable or Disable sudo access. Click **OK**.

If you have a reference host from which you want to provision your bare metal servers, then in the Fetch Properties from Reference Enterprise Manager Host Target section, select **Fetch Properties** to select reference host properties. Select the reference host and the configurations you want to fetch. Specify reference host credentials. The credentials you specify must have root access or you must have sudo privileges set up for the target.

You can choose to use preferred credentials, named credentials, or enter your credentials. If you choose to enter your credentials, specify the user name and password and select the Run Privilege. Choose to **Save Credentials** to use these credentials in future deployments.

Click **Next**.

6. In the Additional OS Details page, specify agent settings, configuration scripts, package selection, and additional operating system configuration, and boot configuration as explained in the tables below.

The Configure Package Selection section displays the packages from the operating component or reference host you specified in the previous screen. You can retain or remove these packages for your provisioning operation.

If you selected an OS component in step 4, these settings will be displayed here. You can edit or retain these values.

Click **Next**.

7. In the Disk Layout page, specify hard disk profile, partition configuration, RAID configuration, Logical Volume Group configuration, and Logical Volume configuration.

To specify the hard disk profile, click **Add**. Specify the **Device Name** and **Capacity**.

To specify the Partition Configuration, click **Add**. Specify the **Mount Point**, **Device Name**, **File System Type**, and **Size (MB)**.

To specify RAID Configuration, click **Add**. Specify the **Mount Point**, **RAID Level**, **Partitions**, and **File System Type**. To configure RAID, ensure that your hard disk has two partitions at the minimum.

To specify the Logical Volume Group Configuration, click **Add**. Specify the **Group Name**, **Partitions**, and **RAIDs**.

To specify the Logical Volume Configuration, click **Add**. Specify the **Mount Point**, **Logical Volume Name**, **Logical Group Name**, **File System Type**, and **Size (MB)**.

If you selected a Disk Layout component in step 4, these settings will be displayed here. You can edit, remove, or retain these values.

Click **Next**.

8. In the Network page, the network properties for the MAC Address or Subnet as specified during target selection, is displayed.

Click **Add** to configure the network interfaces. In the Input Network Interface Properties dialog box, specify the Interface name. Select the **Configuration Type** as:

- Static if you want to specify the IP addresses
- DHCP if you want the DHCP server to assign a network address
- Network Profile if you want to assign network addresses from a network profile.

Select the **Interface Type** as bond master, slave, or non-bonding.

Click **Next**.

9. In the Schedule/Credentials page, provide a schedule for the job, either immediately or at a later date. Specify the Stage Server and Boot Server credentials. You can choose to use preferred credentials, named credentials, or enter your credentials. If you choose to enter your credentials, specify the user name and password and select the Run Privilege. Choose to **Save Credentials** to use these credentials in future deployments.

Click **Next**.

10. In the Review page, verify that the details you have selected are correctly displayed and submit the job for the deployment. If you want to modify the details, click **Back** repeatedly to reach the page where you want to make the changes. Click **Save As Plan** to save the configuration details you have specified. Specify a name and description and click **OK** to save the plan. You can later use the saved plan to provision bare metal boxes.

Click **Submit**.

11. The Deployment Procedure is displayed in the Bare Metal Provisioning page with Status Running. Click on the Status message.
12. In the Procedure Activity page, view the job steps and verify that Status is Success. If the status is Failed, view the steps that have failed, and fix them and resubmit the job.
13. After bare metal systems have been provisioned, verify that they appear in the All Targets page.

Table 23–8 Agent Settings

Element	Description
Install User	User name for installing the agent.
Install Group	Install group for agent.
Agent Registration Password	Specify the password to be used to register the agent with Oracle Management Server.
RPM URL	Agent RPM location.

Table 23–9 Additional OS Configuration

Element	Description
Require TTY	Select this option if you want sudo user to Log in to a separate terminal.
SELinux	You can choose to enable or disable SELinux.
Mount Point Settings	Specify entries for the /etc/fstab file. You can specify mount points on the newly provisioned Linux machine. By default, mount point settings from the reference Linux machine are inherited.
NIS Settings	Specify entries for the /etc/yp.conf file. You can specify NIS settings for the newly provisioned Linux machine. By default, NIS settings from the reference Linux machine are inherited.
NTP Settings	Specify entries for the /etc/ntp.conf file. You can specify NTP settings for the newly provisioned Linux machine. By default, NTP settings from the reference Linux machine are inherited.
Kernel Parameter Settings	Specify scripts for Kernel Parameters.
Initab Settings	Specify settings for /etc/inittab file. All processes are started as part of init operation in boot process. Init operation decides the processes that will start on booting of a machine or when runlevel changes.
Firewall Settings	Specify firewall settings for the Linux target. Firewall settings are disabled by default and can be configured. Make sure that the port used by Management Agent is open for its communication with the Management Service. By default, Management Agent uses port 3872 or a port number in the range 1830-1849, unless configured to use some other port.

Table 23–10 Boot Configuration and Configuration Scripts

Element	Description
Advanced Configuration & Power Interface	Specify settings for boot time parameter for kernel (acpi) in the /boot/grub/grub.conf file.
Use Para-Virtualized kernel	Select if you are using para-virtualized kernel.
Post Install Script	Specify any set of commands that need to be executed on the newly provisioned machine. These commands will be appended to the post section of the kickstart file.
First Boot Script	Specify any set of commands that need to be executed on the newly provisioned machine when it starts up for the first time.

Note: Once Linux is provisioned on the bare metal system, out-of-box Deployment Procedures can be used to provision Database and other Oracle products on the server.

Part VII

Patch Management

This part contains the following chapters:

- [Chapter 24, "Patching Software Deployments"](#)
- [Chapter 25, "Patching Linux Hosts"](#)

Patching Software Deployments

Patching is one of the important phases of the product lifecycle that enables you to keep your software product updated with bug fixes. Oracle releases several types of patches periodically to help you maintain your product. However, patching has always been the most challenging phase of the lifecycle because it is complex, risky, time consuming, and involves downtime. Although you can use several approaches to identify the patches and patch your databases, the challenges still remain the same, unfortunately.

This chapter describes how Oracle Enterprise Manager Cloud Control's (Cloud Control) new patch management solution addresses these patch management challenges. In particular, this chapter covers the following:

- [Overview of the New Patch Management Solution](#)
- [Setting Up Infrastructure for Patching](#)
- [Identifying Patches to Be Applied](#)
- [Applying Patches](#)
- [Diagnosing and Resolving Patching Issues](#)
- [Additional Tasks You Can Perform](#)

24.1 Overview of the New Patch Management Solution

This section describes the following:

- [Overview of the Current Patch Management Challenges](#)
- [Introduction to the New Patch Management Solution](#)
- [Overview of Patch Plans](#)
- [Overview of Patch Templates](#)
- [Supported Targets, Releases, and Deployment Procedures](#)
- [Supported Patching Modes](#)
- [Understanding the Patching Workflow](#)

24.1.1 Overview of the Current Patch Management Challenges

Before you understand the new patch management solution offered by Cloud Control, take a moment to review some of the tools you might be using currently to patch your databases, and the challenges you might be facing while using them ([Table 24-1](#)).

Table 24–1 Current Patch Management Tools and Challenges

Approach	Description	Challenges
OPatch	Oracle proprietary tool that is installed with Oracle products like Oracle Database, Management Agent, SOA, and so on.	<ul style="list-style-type: none"> ■ Difficult to identify the patches to be rolled out ■ Patches only one Oracle home at a time ■ Offers limited support to handle pre and post-patching scripts
Custom Scripts	User-created scripts developed around OPatch, SQLPlus, and so on.	<ul style="list-style-type: none"> ■ Difficult to identify the patches to be rolled out ■ Can be used only on a single server ■ Requires significant maintenance overhead to meet the new version and configuration needs
deployment procedures	Default procedures offered by Cloud Control for automating the patching operations	<ul style="list-style-type: none"> ■ Confusion over which deployment procedure to select ■ Limited scope for validating the patches and targets selected in a deployment procedure ■ Separate deployment procedures for patching in rolling and parallel mode ■ Difficult to handle patch conflicts

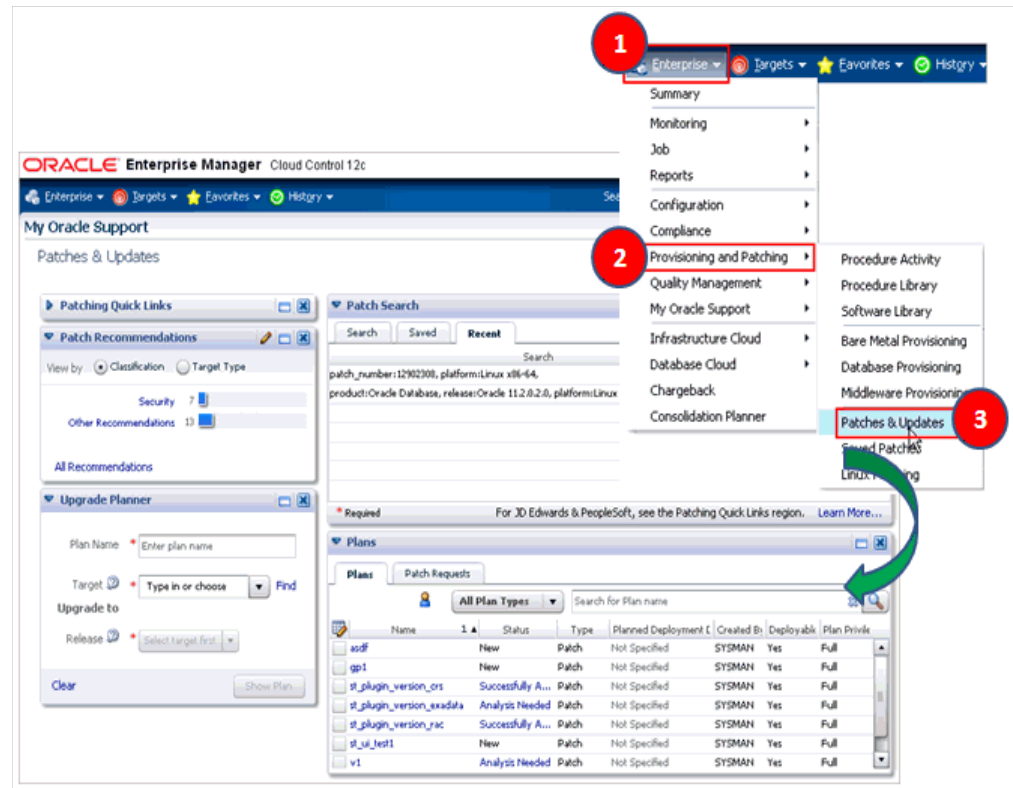
24.1.2 Introduction to the New Patch Management Solution

Cloud Control addresses the challenges described in [Section 24.1.1](#) with its much-improved patch management solution that delivers maximum ease with minimum downtime. The new patch management solution offers the following benefits:

- Integrated patching workflow with My Oracle Support, therefore, you see recommendations, search patches, and roll out patches all using the same user interface.
- Complete, end-to-end orchestration of patching workflow using *Patch Plans*, including automated selection of deployment procedures and analysis of the patch conflicts, therefore, there is minimal manual effort required. For more information on patch plans, see [Section 24.1.3](#).
- Clear division of responsibilities between designers and operators - Designers can focus on creating patch plans, testing them on a test system, and saving them as patch templates. Operators can focus on creating patch plans out of the template for rolling out the patches on a production system.
- Easy review of patches for applicability in your environment, validation of patch plans, and automatic receipt of patches to resolve validation issues.
- Saving successfully analyzed or deployable patch plans as patch templates, which contain a predetermined set of patches and deployment options saved from the source patch plan.
- Out-of-place patching for standalone (single-instance) database targets and Oracle Grid Infrastructure targets that are part of Oracle Exadata.
- Flexible patching options such as rolling and parallel, both in offline and online mode.

Figure 24–1 shows you how you can access the Patches and Updates screen from within Cloud Control console.

Figure 24–1 Accessing the Patches & Updates Screen



24.1.3 Overview of Patch Plans

This section describes the following:

- [Introduction to Patch Plans](#)
- [Types of Patch Plans](#)
- [Introduction to Create Plan Wizard](#)

24.1.3.1 Introduction to Patch Plans

Patch plans help you create a consolidated list of patches you want to apply as a group to one or more targets. Patch plans have states (or status) that map to key steps in the configuration change management process. Any administrator or role that has view privileges can access a patch plan.

Patch plan supports the following types of patches:

- Patch Sets

Note:

- Patch Sets for Oracle Database Release 10g Release 2 (10.2.0.x) and Release 11g Release 1 (11.1.0.x). However, note that Patch Sets for Oracle Database Release 11g Release 2 (11.2.0.x) are complete installs (or full releases) and you must use the Database Upgrade feature to install them as they follow out-of-place patching approach.
 - Patch Sets are not supported on Oracle WebLogic Server targets, Oracle Fusion Application targets, and Oracle SOA Infrastructure targets.
-
-

- Patches (One-Off)
 - Interim Patches that contain a single bug fix or a collection of bug fixes provided as required. Also include one-offs for customer-specific security bug fixes.
 - Diagnostic Patches, intended to help diagnose or verify a fix or a collection of bug fixes.
 - Patch Set Updates (PSU), contain a collection of high impact, low risk, and proven fixes for a specific product or component.
 - Critical Patch Updates (CPU), contain a collection of security bug fixes.
-
-

Note: You cannot add both patch sets and patches to a patch plan. Instead, you can have one patch plan for patch sets, and another patch plan for patches.

A patch can be added to a target in a plan only if the patch has the same release and platform as the target to which it is being added. You will receive a warning if the product for the patch being added is different from the product associated with the target to which the patch is being added. The warning does not prevent you from adding the patch to the plan.

You can include any patch for any target in a plan. The plan also validates Oracle Database, Fusion Middleware, and Cloud Control patches against your environment to check for conflicts with installed patches.

The patch plan, depending on the patches you added to it, automatically selects an appropriate deployment procedure to be used for applying the patches. For information on the patching deployment procedures used for various database target types, see [Table 24-2](#).

Note:

- Patch plans are currently not available for hardware system or operating system patching.
- Any administrator or role that has view privileges can access a patch plan. For information on roles and privileges required for patch plans and patch templates, see [Section 24.2.2](#).
- If you are patching an Oracle Grid Infrastructure target, which is part of Oracle Exadata, then you can add only one patch (Oracle Exadata patch) per patch plan. For all other target types, you can add as many patches as you want, as long as the patches are of the same release and platform as the targets being patched.

24.1.3.2 Types of Patch Plans

A patch plan can be either deployable or nondeployable.

- A patch plan is deployable when:
 - It contains only patches of the same type (homogenous patches).
 - It contains targets that are supported for patching, similarly configured, and are of the same product type, platform, and version (homogeneous targets).
 - There are no other conflicts within the plan.
- A patch plan that does not meet any of the conditions listed for a deployable plan is a nondeployable plan. If your patch plan is not deployable, you cannot deploy the patches using the patch plan, but you can perform some analysis and checks, download the patches, and manually apply the them.

24.1.3.3 Introduction to Create Plan Wizard

[Figure 24–2](#) shows the Create Plan Wizard that enables you to create, view, and modify patch plans.

Figure 24–2 Create Plan Wizard

The screenshot displays the 'Step 1: Plan Information' screen of the Create Plan Wizard. On the left, a vertical sidebar lists five steps: 1 Plan Information (selected), 2 Patches, 3 Deployment Options, 4 Validation, and 5 Review & Deploy. The main content area is titled 'Step 1: Plan Information' and features a checkbox labeled 'Plan is deployable' which is checked. Below this, a text box explains that plans can be saved and referenced while working out details. An 'Overview' section contains the following fields: 'Name' with the value 'Database_patches', 'Planned Deployment Date' set to 'Nov 4, 2011 12:00 am', 'Description' with the text 'To patch standalone database targets', and 'Created By' set to 'DESIGNER'. At the bottom of the wizard, there are four buttons: 'Exit Wizard', 'Back', 'Next', and 'Review'.

The wizard has the following screens:

Screen 1: Plan Information

Enables you to provide basic information about the plan, such as a unique name for the plan, a planned deployment date, a brief description. Also enables you to add an administrator or a role that can access the patch plan.

Screen 2: Patches

Enables you to view the patches already part of the patch plan, and manually add additional patches to the plan and associate targets that need to be patched.

Screen 3: Deployment Options

Enables you to configure the patch plan with deployment options that suit your needs. Although this step is common for all target types, the deployment options offered by this step depend on the target types selected in the patch plan.

For all target types, you can select a customized deployment procedure for deploying the patches, and specify the credentials to be used. For database targets, you can specify a nondefault staging location for storing patches and skip the staging process if the patches are already staged. For standalone databases, you can choose between out-of-place patching and in-place patching. For Oracle RAC databases and Oracle Grid Infrastructure targets, you can choose to apply the patches in rolling or parallel mode in order to control the downtime of the system.

Screen 4: Validation

Enables you to validate the patch plan and determine whether the patches can be rolled out without any issues. Essentially, it enables you to perform the following checks using the patch information from Oracle, the inventory of patches on your system (gathered by the configuration manager), and the information from candidate patches.

- Patch Conflict Checks
 - Conflict between the patches added to the patch plan and the patches already present in the Oracle home
 - Conflict among patches within the patch plan
- Target Sanity Checks
 - Target status and configuration checks
 - OPatch and OUI checks
 - Inventory sanity checks, such as locks, access, and so on
 - Hard disk space checks
 - Cluster verification checks (cluvfy, srvctl config)
 - SQLPlus checks (with sample SQL)

Note: For Oracle WebLogic targets, instead of the OPatch and OUI check, you must perform the SmartUpdate version check.

In addition to checking for conflicts, it enables you to check for patch conflicts between the patches listed in the plan.

Screen 5: Review & Deploy

Enables you to review the details you have provided for the patch plan, and then deploy the plan. The page also enables you to review all the impacted targets so that you understand what all targets are affected by the action you are taking.

24.1.4 Overview of Patch Templates

This section describes the following:

- [Introduction to Patch Templates](#)
- [Introduction to Edit Template Wizard](#)

24.1.4.1 Introduction to Patch Templates

Patch templates are another important aspect of the patch management solution. Patch templates help you create predesigned plans based on an existing successfully analyzed or deployable patch plan, however without any targets selected. A patch template contains a predetermined set of patches and deployment options saved from the source patch plan, and enables you to select a completely new set of targets.

This way, as a *Patch Designer*, you can create a patch plan with a set of patches, test them in your environment, save the successfully analyzed patch plan as a patch template, and publish them to *Patch Operators*. As a *Patch Operator*, who can create patch plans out of the templates, add another set of targets, and roll out the patches to the production environment in a recursive manner.

This way, you reduce the time and effort required to create new patch plans, and as a *Patch Designer*, you expose only the successfully analyzed and approved plans to *Patch Operators*.

Note: An administrator or role that has the privileges to create a patch template and view a patch plan, which is being used to create a template, can create a patch template.

24.1.4.2 Introduction to Edit Template Wizard

Figure 24–3 shows the Edit Template Wizard that enables you to view the contents of a patch plan template and modify the description.

Figure 24–3 Create Plan Template Wizard

The screenshot displays the 'Step 1: Plan Information' screen of the 'Create Plan Template Wizard'. On the left, a vertical navigation pane shows three steps: '1 Plan Information' (selected), '2 Patches', and '3 Deployment Options'. Below the steps is a legend for a red asterisk indicating a 'Required Field'. The main content area contains the following information:

- Step 1: Plan Information**
- Templates are useful for applying a successful patch plans to multiple targets. Use the **Create Plan** button to create a new plan based on this template.
- Overview**
- Name:** * WebLogic Server Patch Template (Required field)
- Planned Deployment Date:** Not Set
- Description:** To patch Oracle WebLogic Server targets.
- Created By:** DESIGNER

At the bottom of the wizard, there are five buttons: 'Exit Wizard', 'Create Patch Compliance Framework', 'Back', 'Next', and 'Create Plan'.

When you view or modify a patch plan template, the Patch Plan Template opens. The wizard has the following screens:

Screen 1: General Information

Enables you to view general information about the template, and modify the description and the deployment date.

Screen 2: Patches

Enables you to view a list of patches part of the patch plan template. The patches listed here are the patches copied from the source patch plan that you selected for creating the template.

Screen 3: Deployment Options

Enables you to view the deployment options configured in the patch plan template.

24.1.5 Supported Targets, Releases, and Deployment Procedures

Table 24–2 lists the targets and their releases you can patch on different platforms using the new patch management solution, and the default deployment procedures that the patch plans automatically select depending on the target type. The deployment procedures are supported only through patch plans. Although they are exposed in the deployment procedure Manager page, you cannot select and run them independently; you must always create a patch plan to run them.

Note: You need to meet the following prerequisites before patching Oracle WebLogic Server targets:

1. Ensure that you have applied the Enterprise Manger Bundle Patch 1 on the OMS and the Management Agents monitoring the Oracle WebLogic Server targets.
 2. Ensure that you have applied MOS 12.1.0.2 plug-in on the OMS. This must be applied to all of the OMS instances in a multi-OMS environment.
 3. Ensure that you have applied Oracle Fusion Middleware 12.1.0.2 plug-in on the OMS and the Management Agent monitoring the Oracle WebLogic Server targets.
-
-

Table 24–2 Supported Targets and Releases for Patching

Supported Target Type	Supported Targets and Releases	Supported Platform	Supported Default deployment procedure
Oracle Database	Oracle Database (standalone) 10g Release 1 to 11g Release 2	All Platforms	Patch Oracle Database
	Oracle Automated Storage Management (Oracle ASM) 10g Release 1 to 11g Release 2	All Platforms	Patch Standalone Oracle ASM
	Oracle Real Application Cluster (Oracle RAC) 10g Release 1 to 11g Release 2	All Platforms	<ul style="list-style-type: none"> ■ Patch Oracle RAC Database - Rolling ■ Patch Oracle RAC Database - All Nodes
	Oracle Exadata RAC Databases ¹ 11g Release 2 (11.2.0.1, 11.2.0.2, and 11.2.0.3)	All Platforms	<i>No default deployment procedure; it is built dynamically</i>
	Oracle Restart 10g Release 1 to 11g Release 2	All Platforms	Patch Oracle Restart
	Oracle Clusterware 10g Release 1 to 11g Release 1	All platforms except for Microsoft Windows	<ul style="list-style-type: none"> ■ Patch Oracle Clusterware - Rolling ■ Patch Oracle Clusterware - All Nodes
	Oracle Grid Infrastructure 11g Release 2	All Platforms	<ul style="list-style-type: none"> ■ Patch Oracle Clusterware - Rolling ■ Patch Oracle Clusterware - All Nodes
Oracle WebLogic Server	Oracle WebLogic Server 10g Release 3 (10.3.1), (10.3.2), (10.3.3), (10.3.4), (10.3.5), (10.3.6), and 12c Release 1 (12.1.1)	All Platforms	<ul style="list-style-type: none"> ■ Patch Oracle WebLogic Server In Parallel Mode ■ Patch Oracle WebLogic Server In Rolling Mode
Oracle Fusion Applications	Oracle Fusion Applications 11g Release 1 (11.1.1.5.1) and (11.1.2.0.0) (RUP1)	All Platforms	Patch Oracle Fusion Applications
Oracle Application Server	Oracle Application Server 10g Release 1	All Platforms	Patch Application Server
Oracle SOA Infrastructure	Oracle SOA Infrastructure 11g Release 1 (11.1.1.1.0 - 11.1.1.6.0)	All Platforms	<ul style="list-style-type: none"> ■ Patch Oracle SOA Infrastructure In Parallel Mode ■ Patch Oracle SOA Infrastructure In Rolling Mode

¹ Exclusively tested for Oracle Exadata Database Machine recommended bundle patches.

Note: You can also patch primary and standby databases configured with Oracle Data Guard. However, to patch such targets, you must use a customized patching deployment procedure. For more information, see [Section 24.6.12](#).

24.1.6 Supported Patching Modes

This section describes the following patching modes:

- [Patching in Online and Offline Mode](#)
- [Patching in In-Place and Out-of-Place Mode](#)
- [Patching in Rolling and Parallel Mode](#)

24.1.6.1 Patching in Online and Offline Mode

You have the flexibility to choose between online and offline modes of patching.

Online Mode

Online Mode is useful when Cloud Control can connect to My Oracle Support using an Internet connection. Using this mode, you can see recommendations from Oracle for the patches to be applied, and manually search patches directly on My Oracle Support and add them to your patch plan. In addition, you can access community information, knowledge articles, service requests, and so on, and also automatically resolve patch conflicts with a merge patch directly from My Oracle Support.

Offline Mode

Offline Mode is useful when Cloud Control cannot connect to My Oracle Support. Using this mode, you can search patches that were manually uploaded to the Software Library, and add them to your patch plan. In offline mode, you cannot do the following:

- Search and download patches from My Oracle Support
- View additional information about the patch
- Access community information, knowledge articles, service requests
- View the Related Activity region

Note: By default, the patching mode is set to online. If you want to switch the mode to offline, then from the **Setup** menu, select **Proxy Settings**. On the Patching Setup page, click the **Online and Offline Settings** tab, and in the Settings section, select **Offline**.

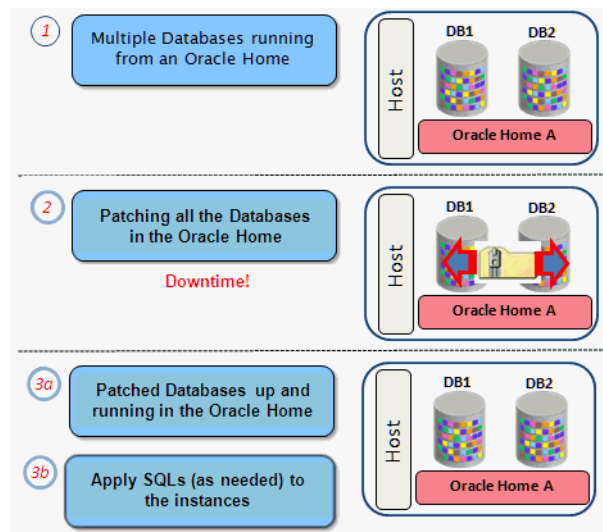
24.1.6.2 Patching in In-Place and Out-of-Place Mode

You have the flexibility to choose between in-place and out-of-place patching modes.

In-Place Mode

In-place mode of patching is a patching mechanism where you directly patch the database home. In this mode, before applying the patch, you actually bring down all the database instances running out of that database home, which means there will be a downtime. And after applying the patch, you restart all the database instances. All database instances will and must be patched in the same manner. Note that in this mode, recovery takes longer if there is a problem because the Oracle home that you patched is the original database home, not its copy.

Figure 24-4 illustrates how multiple database instances running from an Oracle home get patched in-place patching mode.

Figure 24–4 In-Place Mode of Patching**Out-of-Place Mode**

Out-of-place mode of patching is a patching mechanism that clones the existing database home, and patches the cloned home instead of the original home. Once the cloned home is patched, you can migrate the database instances to run from the cloned home, which means there will be minimal downtime while switching over the instances, but not a significant downtime.

Note: Out-of-place mode of patching is currently supported only for standalone (single-instance) databases targets and Oracle Grid Infrastructure targets that are part of Oracle Exadata. For more information on how the patching is performed, see [Section 24.4.7](#).

While migrating the database instances, you can choose to migrate all of the instances or only some of them depending on the downtime you can afford to have in your data center. If you choose to migrate only a few instances in one session, then ensure that you migrate the rest in the next session. This way, you can control the downtime in your data center as you divide the migration activity. This is particularly useful when you have multiple database instances running out of an Oracle home.

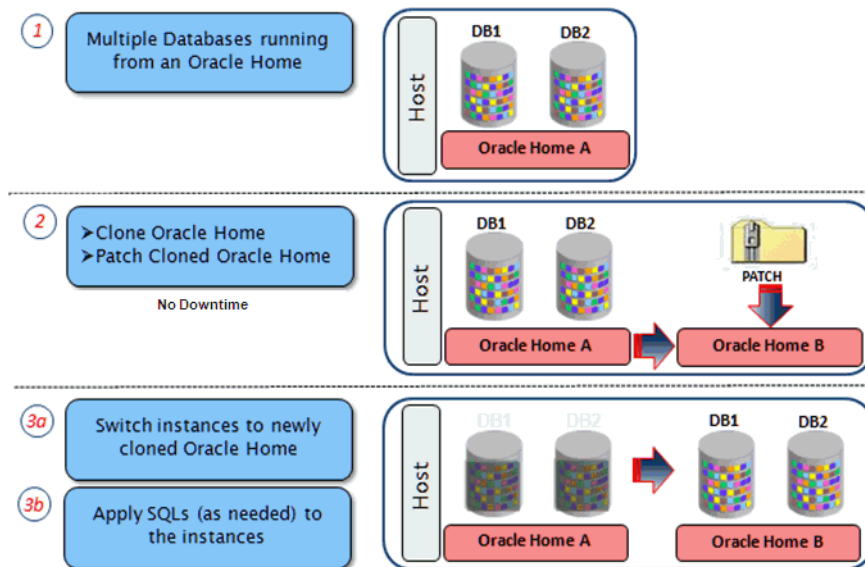
Note: You select the database instances you want to migrate, in the patch plan. The selected database instances are migrated when the patch plan is in the *Deploy* state. If you selected only a few instances to be migrated, then to migrate the remaining instances, create another patch plan, on the Deployment Options page, select the existing home, and then select the remaining instances that need to be migrated.

Oracle always recommends out-of-place patching because the downtime is minimal and recovery in case of a problem is easy; you can always switch back to the original database home in case of a problem with the clone home.

Note: If you patched an Oracle Grid Infrastructure target, which is part of Oracle Exadata, in out-of-place patching mode, then you can switch back to the original home directly from the Create Plan Wizard—the wizard provides a **Switchback** button that enables you to perform the operation. However, this button is not available for any other target type.

Figure 24–5 illustrates how multiple database instances running from an Oracle home get patched in out-of-place patching mode.

Figure 24–5 Out-of-Place Mode of Patching



24.1.6.3 Patching in Rolling and Parallel Mode

While patching Oracle Real Application Cluster (Oracle RAC) targets, Oracle Grid Infrastructure targets (whether or not they are part of Oracle Exadata), Oracle WebLogic Server targets, Oracle Fusion Application targets, or Oracle SOA Infrastructure targets you can choose to patch the instances of the cluster either in rolling or parallel mode.

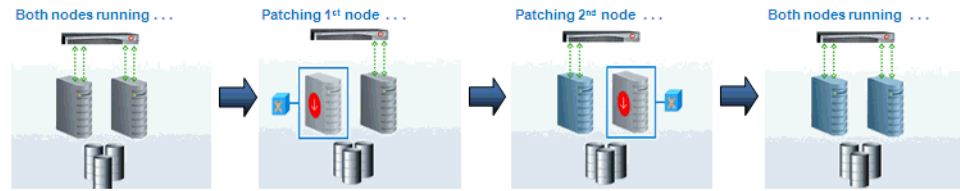
Rolling Mode

Rolling Mode refers to the patching methodology where the nodes of the cluster are patched individually, that is, one by one. For example, if you are patching a clusterware that has five nodes, then the first node is shut down, patched, and restarted, and then the process is rolled over to the next node until all the nodes are patched successfully.

Note: The ReadMe of the patch clearly states whether or not you can use the *Rolling Mode* to apply your patches. Therefore, use this mode only if it is stated in the ReadMe.

Figure 24–6 illustrates how a two-node Oracle RAC gets patched when rolling mode is used.

Figure 24–6 Rolling Mode of Patching

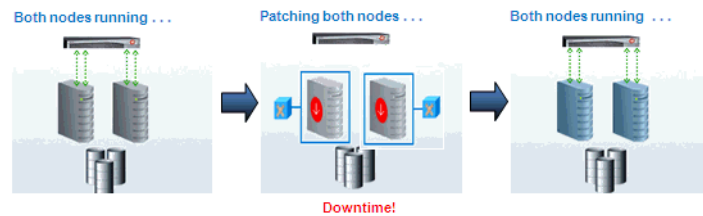


Parallel Mode

Parallel Mode refers to the patching methodology where all the nodes are patched at a time, collectively. In this methodology, all the nodes are shut down and the patch is applied on all of them at the same time.

Figure 24–7 illustrates how a two-node Oracle RAC gets patched when parallel mode is used.

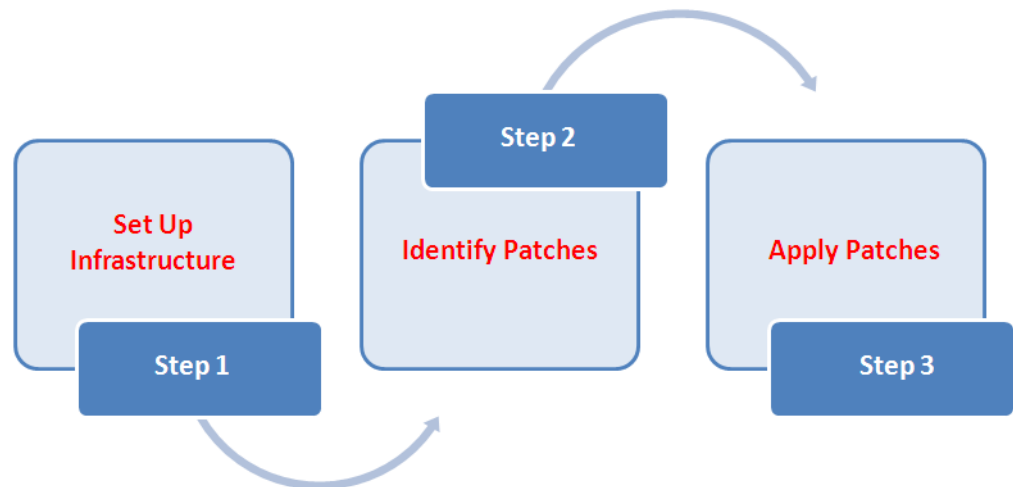
Figure 24–7 Parallel Mode of Patching



Note: For all other database target types, the default patching mode is rolling mode.

24.1.7 Understanding the Patching Workflow

The following illustration describes the overall workflow of the patch management solution offered through the integrated functionality within the Cloud Control console.



Step	Step Name	Description	Reference Links
Step 1	Set Up Infrastructure	Meet the prerequisites and set up the infrastructure for rolling out patches. Essentially, create admin roles for creating <i>Patch Plans</i> and <i>Patch Templates</i> , meet other mandatory and optional prerequisites, make online or offline patching settings.	Section 24.2, "Setting Up Infrastructure for Patching"
Step 2	Identify the Patches	View the recommendations made by Oracle on the patches to be applied, and identify the ones you want to apply. Access community information (from innumerable customers).	Section 24.3, "Identifying Patches to Be Applied"
Step 3	Apply Patches	Create patch plans with patches and associated targets, perform prerequisite checks, analyze the patches for conflicts and resolve the issues, and then save the successfully analyzed plan as a patch template. Then, create a new patch plan out of the patch template and use that to deploy the patches in your environment.	Section 24.4, "Applying Patches"

24.2 Setting Up Infrastructure for Patching

This section describes how you can set up the infrastructure for patching. Meet these prerequisites before you start rolling out the patches.



This section is mainly for **Patch Administrators** or **Patch Designers** who want to keep the infrastructure ready for rolling out patches. This is mostly a one-time task if you have decided on the way (online or offline) you want to patch.

This section covers the following:

- [Meeting Basic Infrastructure Requirements](#)
- [Creating Administrators with the Required Roles](#)
- [Setting Up Infrastructure for Patching in Online Mode \(Connected to MOS\)](#)
- [Setting Up Infrastructure for Patching in Offline Mode \(Not Connected to MOS\)](#)

24.2.1 Meeting Basic Infrastructure Requirements

Meet the basic infrastructure requirements as described in [Chapter 2](#). The chapter describes both mandatory and optional requirements.

24.2.2 Creating Administrators with the Required Roles

[Table 24–3](#) describes the roles and the minimum privileges required for using patch plans and patch templates. These roles are default roles available in Cloud Control. You need not create them, but you must explicitly create administrators based on these roles. For instructions, see [Section 2.4](#).

Table 24–3 Roles and Privileges for Using Patch Plans and Patch Templates

Role	Patch Plan Scope	Patch Template Scope	Patch Plan and Patch Templates Privileges	Target Privileges	Resource Privileges	Implementation Recommendation
Patch Administrator	Create, View, Modify, Delete	Create, View, Modify, Delete	FULL_ANY_PATCH_PLAN FULL_ANY_PLAN_TEMPLATE GRANT_PRIV_PATCH_PLAN	Operator any Target <i>(alternatively, you can select a particular target you want to patch and grant operator privilege to it)</i>	<ul style="list-style-type: none"> ▪ Resource Type: deployment procedure Privilege: Create ▪ Resource Type: Job System Privilege: Create ▪ Resource Type: Software Library Entity Privilege: Manage Any Software Library Entity 	Required if you want to create and manage <i>Patch Designer</i> and <i>Patch Operator</i> roles. You can also create these roles directly as a SUPER ADMIN or SYSMAN.
Patch Designer	Create, View	Create, View	FULL_PATCH_PLAN FULL_PLAN_TEMPLATE	- do -	- do -	Required when you want to grant the access and also have restrictions. Alternatively, you can create an EM user with <i>Patch Designer</i> role.
Patch Operator	Create	View	CREATE_PATCH_PLAN VIEW_ANY_PLAN_TEMPLATE	- do -	- do -	- do -

24.2.3 Setting Up Infrastructure for Patching in Online Mode (Connected to MOS)

If you choose to patch your targets when Cloud Control is online, that is, when it is connected to My Oracle Support, then meet the following setup requirements:

- [Enabling Online Mode](#)
- [Setting Up Network Proxy and Realm Configuration Settings](#)

24.2.3.1 Enabling Online Mode

Note: This is the default mode for patching in Cloud Control. Therefore, you do not have to manually set this up the first time. However, if you have set it to offline mode for a particular reason, and if you want to reset it to online mode, then follow the steps outlined in this section.

To patch the targets in online mode, you must set the connection setting in Cloud Control to Online mode. To do so log in with Super Administrator privileges, and follow these steps:

1. From the **Setup** menu, select **Proxy Settings**.

2. On the Proxy Settings page, click the **Online and Offline Settings** tab.
3. On the Online and Offline Settings tab, in the Settings section, select **Online**.

24.2.3.2 Setting Up Network Proxy and Realm Configuration Settings

In online mode, Cloud Control connects to My Oracle Support to download patches, patch sets, ARU seed data such as products, platforms, releases, components, certification details, and patch recommendations. For this purpose, Cloud Control uses the Internet connectivity you have on the OMS host to connect to My Oracle Support. However, if you have a proxy server set up in your environment, then you must register the proxy details.

Besides connecting to My Oracle Support, Cloud Control requires Internet connectivity between the OMS and the Management Agents, so the Management Agents can upload configuration details via the OMS to the Management Repository. However, if the OMS and the Management Agents are in different network domains with the same or different proxy servers set up, then you must register the proxy details.

To register the proxy server settings for OMS, follow these steps:

1. From the **Setup** menu, select **Proxy Settings**.
2. On the My Oracle Support and Proxy Connection tab, do the following:
 - a. In the My Oracle Support section, by default, **Patch Search URL** displays <https://updates.oracle.com> as the URL where the patches will be searched. If you want to verify the connectivity to My Oracle Support, then click **Test**.

If the credentials are valid and if Cloud Control is able to connect to My Oracle Support successfully, then a status message is displayed to this effect.
 - b. In the My Oracle Support Connection Setting section, select **Manual Proxy Configuration**. Enter the proxy settings for the HTTPS protocol—enter the name of the proxy server, the port, the realm (if the credentials are configured for realm), and the credentials (if the credentials are required for authentication).

Note: Ensure that your proxy allows connectivity to aru-akam.oracle.com, ccr.oracle.com, login.oracle.com, support.oracle.com, and updates.oracle.com.

NTLM (NT LAN Manager) based Microsoft Proxy server is not supported. To enable access add the above URLs to the Unauthenticated Sites Properties of the NTLM/Microsoft Proxy server.

The Connection Configuration subsection shows the default values set for **Timeout** and **Number of Retries**. Timeout indicates the time in milliseconds after which it should automatically time out if the connection takes unusually long time to connect to My Oracle Support. Number of Retries indicates the number of times it should retry connecting to My Oracle Support after timing out. Change the default values to higher values only if required.

- c. In the Agent Connection Setting section, select the settings to be considered for all Management Agent-related communications.

If you want to use the settings specified in the My Oracle Support Connection String, then select **Use My Oracle Support Connection Settings**.

If you want to enter a new set of proxy details, then select **Manual Proxy Configuration** and, provide the details for HTTPS protocol. Specify the name of the proxy server, port, sites for which proxy must not be used, realm (if credentials are configured for realm), and credentials (if credentials are required for authentication).

Note: REALM is mandatory if the authentication credentials are required to access the proxy server. Check with your network administrator for the correct value.

- d. In the Test URL section, to verify whether the Management Agent is reachable, specify a valid Management Agent URL and click **Test**. If the URL is valid and if Cloud Control is able to reach the Management Agent successfully, then a status message is displayed to this effect.
- e. Click **Apply**.

24.2.4 Setting Up Infrastructure for Patching in Offline Mode (Not Connected to MOS)

If you choose to patch your targets when Cloud Control is offline, that is, when it is not connected to My Oracle Support, then meet the following setup requirements:

- [Enabling Offline Mode](#)
- [Downloading Enterprise Manager Catalog Zip File From Another Host With Internet Connectivity](#)
- [Uploading Enterprise Manager Catalog Zip File from your Host With No Internet Connectivity](#)
- [Creating "Refresh From My Oracle Support" Job](#)
- [Uploading OPatch Patches to Oracle Software Library](#)
- [Uploading Patches to Oracle Software Library](#)

24.2.4.1 Enabling Offline Mode

To patch the targets in offline mode, you must set the connection setting in Cloud Control to offline mode. To do so, follow these steps:

1. From the **Setup** menu, select **Proxy Settings**.
2. On the Proxy Settings page, click the **Online and Offline Settings** tab.
3. On the Online and Offline Settings tab, in the Online and Offline section, select **Offline**.

24.2.4.2 Downloading Enterprise Manager Catalog Zip File From Another Host With Internet Connectivity

In offline mode, you must use another host that has Internet connection and manually download the `em_catalog.zip` files from My Oracle Support. Use the following URL to download the latest catalog file:

https://updates.oracle.com/download/em_catalog.zip

The information about the targets affected by the latest patches, and the patch you have to manually download is available in the catalog zip file.

24.2.4.3 Uploading Enterprise Manager Catalog Zip File from your Host With No Internet Connectivity

After downloading the metadata XML files as described in the preceding section, ensure that you transfer the download (latest) `em_catalog.zip` file back to your host machine using FTP or any other file transfer methodology. From your local host, you can then log into Enterprise Manager Cloud Control to upload the zip file. To do so, follow these steps:

1. From the **Setup** menu, select **Proxy Settings**.
2. On the Proxy Settings page, click the **Online and Offline Settings** tab.
3. On the Online and Offline Settings tab, in the Online and Offline section, click **Browse** to upload the latest `em_catalog.zip` file to the Management Repository. Wait for the files to get uploaded properly.

24.2.4.4 Creating "Refresh From My Oracle Support" Job

Once the Enterprise Manager Catalog zip (`em_catalog.zip`) file is uploaded as described in the preceding section, a default, dedicated job called *Refresh From My Oracle Support* is run periodically for the following reasons:

- To extract information from the metadata XML files and display them in Cloud Control.
- To update the metadata tables with information about new products, releases, certifications, and so on.

However, if you want to extract the information from the metadata files immediately after uploading the files, that is, on an on-demand basis, then you must create a new *Refresh From My Oracle Support* job.

Note:

- In offline mode, the job does not actually connect to My Oracle Support. Instead, it looks for the metadata XML files you manually downloaded and stored in the Management Repository to compute the patch recommendations.
 - In online mode, the job actually connects to My Oracle Support and automatically downloads the metadata XML files, and then computes the patch recommendations based on the inventory information collected.
-
-

To create a new *Refresh From My Oracle Support* job, follow these steps:

1. From the **Enterprise** menu, select **Job**, then select **Activity**.
2. On the Job Activity page, from the **Create Job** list, select **Refresh From My Oracle Support** and click **Go**.
Cloud Control displays the Create 'Refresh From My Oracle Support' Job page.
3. On the Create 'Refresh From My Oracle Support' Job page, enter a name for this job, schedule it to run immediately, and grant access to roles that must have access to this job.
4. Click **Submit**.

24.2.4.5 Uploading OPatch Patches to Oracle Software Library

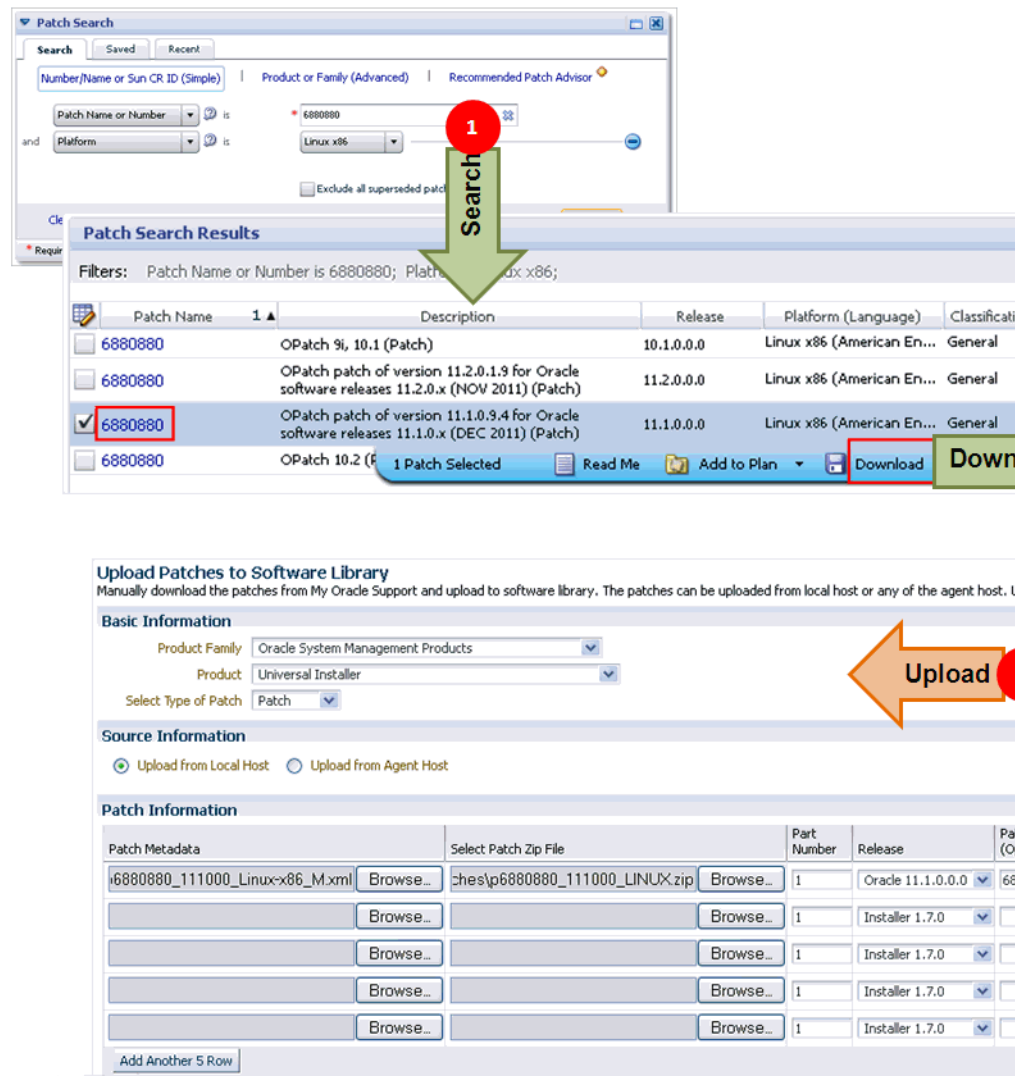
From My Oracle Support, manually download patch 6880880 and its metadata file to a host monitored by Cloud Control (essentially, that host must have a Management Agent installed.) Ensure that you download the patch for the required platform and the version of the target you are patching. This is a platform-specific patch, so you will have to carefully select the platform while downloading this patch.

Note: Unlike OUI installed products, Oracle WebLogic Server uses SmartUpdate tool for patching its targets. To ensure that you have the latest version of the SmartUpdate tool in your environment, you need to download patch 12426828, and its metadata file to a host monitored by Cloud Control.

Then, upload it to the Software Library as described in [Section 24.2.4.6](#). While uploading the patch using the Upload Patches to Software Library page, in the Basic Information section, ensure that you select **Oracle System Management Products** as the Product Family and **Universal Installer** as the Product List.

[Figure 24–8](#) illustrates how you can download the 11.1.0.0.0 release of patch 6880880 for Linux x86 platform, and upload it to the Software Library for patching Oracle Database 11g Release 1 (11.1.0.0.0) that is running on Linux x86.

Figure 24–8 Downloading OPatch Patch from My Oracle Support and Uploading It to Oracle Software Library



24.2.4.6 Uploading Patches to Oracle Software Library

For patching targets in offline mode, you must have already stored the patches and their metadata files in the Software Library so that they can be searched, selected, and added to the patch plans from the Software Library.

For this purpose, you must first manually download the patches and their metadata files from My Oracle Support, and then upload them to the Software Library. While uploading the patches and their metadata files, you must enter some information related to the patches in the Upload Patches to Software Library page, so while downloading the patches from My Oracle Support, Oracle recommends you to identify and make note of all the required details.

This section describes the following:

- [Downloading a Patch from My Oracle Support and Identifying the Details Required for Uploading a Patch to Software Library](#)
- [Uploading a Patch to the Software Library](#)

24.2.4.6.1 Downloading a Patch from My Oracle Support and Identifying the Details Required for Uploading a Patch to Software Library To download a patch and its metadata file from My Oracle Support, and to identify the details that you need to provide while uploading a patch to the Software Library, follow these steps:

1. Log in to My Oracle Support, and click the **Patches & Updates** tab.
2. On the Patches & Updates page, in the Patch Search section, enter the patch number you want to search for as shown in [Figure 24–9](#), and click **Search**.

Figure 24–9 Searching Patch

The screenshot shows the 'Patch Search' window with the following details:

- Search tabs: Search, Saved, Recent
- Search criteria: Patch Name or Number is 12582664 and Platform is Linux x86-64
- Buttons: Clear, Save, Search
- Footer: * Required For JD Edwards & PeopleSoft, see the Patching Quick Links region. Learn More...

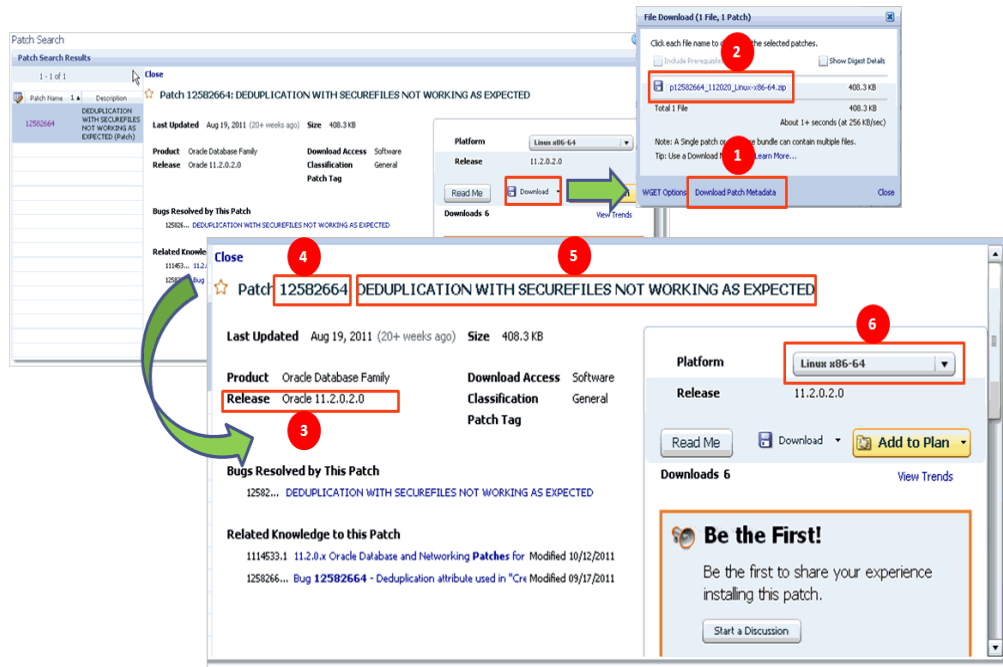
3. On the Patch Search Results page, click the patch number. Cloud Control displays details of the patch in a collapsible frame as shown in [Figure 24–10](#).

Also click **Download** and select **Desktop**. In the File Download dialog, click **Download Patch Metadata**, and then in the Download Patch Metadata dialog, click **Download** to download the patch metadata file as shown in [Figure 24–10](#).

Note: Oracle recommends that you transfer the patch ZIP file and the metadata XML file to the Management Agent host, where the Management Agent could be an agent on an OMS machine, or on the target host. Upload these files from the Management Agent host to the Software Library.

Make a note of the details highlighted in [Figure 24–10](#). You will need to enter these details on the Upload Patch page while uploading the patch.

Figure 24–10 Identifying Patch Details



24.2.4.6.2 Uploading a Patch to the Software Library To upload a patch to the Software Library, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Saved Patches**.
2. On the Patching page, click **Upload**.
3. On the Upload Patches to Software Library page, in the Basic Information section, do the following:

- a. From the **Product Family** list, select the product family for which you are uploading the patch as shown in [Figure 24–11](#).

For example, if you want to patch an Oracle WebLogic Domain, then select the product family it belongs to, that is, **Oracle Fusion Middleware**. You must have made a note of this information according to Step (3) of [Section 24.2.4.6.1](#).

- b. From the **Product** list, select the product for which you are uploading the patch. For example, select **Oracle WebLogic Server**.
- c. From the **Select Type of Patch**, select either **Patch** or **Patch Set** depending on the type of patch you are uploading.

Patch Sets are not supported on Oracle WebLogic Server targets.

4. In the Source Information section, do the following:
 - Select **Upload from Agent Host**.

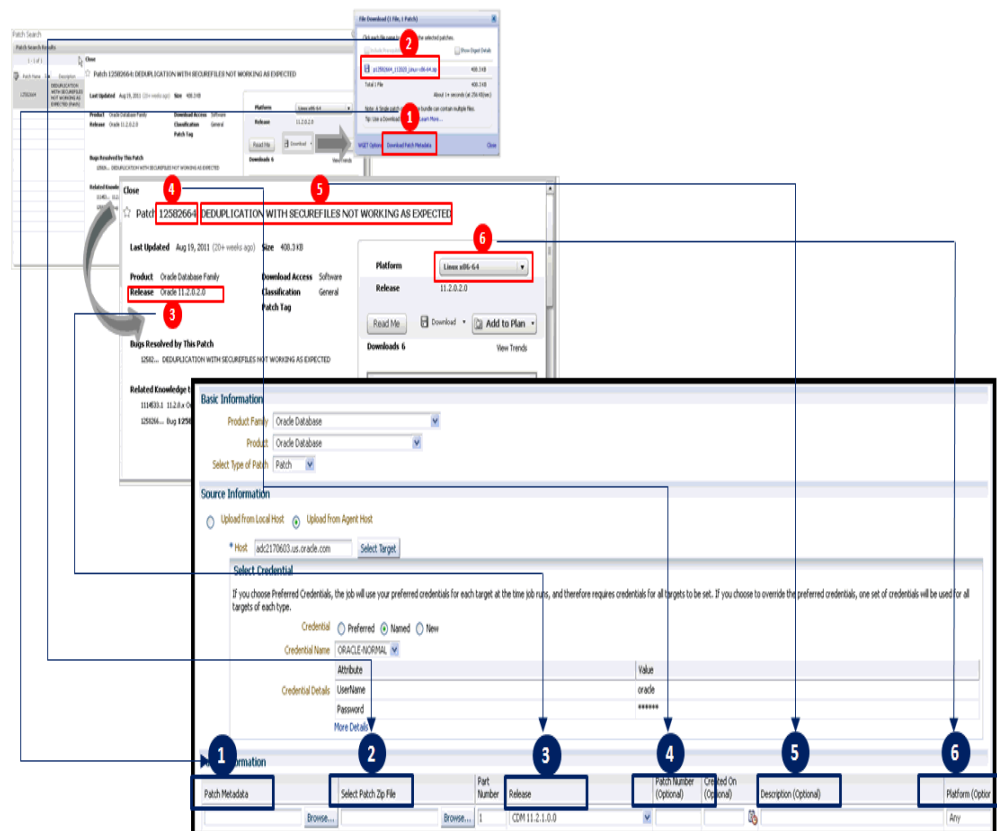
- Click **Select Target** and select the name of the agent host where the patches are temporarily stored.
 - In the Select Credential subsection, select **Named**, and from the **Credential Name** list, select the named credential you want to use to access the agent host.
5. In the Patch Information section, enter the absolute path to the patch metadata XML file and the patch ZIP file, and provide details of the patch in the other columns—part number, release, patch number, creation date, description, platform, and language—as shown in [Figure 24–11](#).

Note: Part number identifies multiple files of the same patch. For example, Patch 6890831 has two zip files, p6890831_111070_AIX5L_1of2.zip (Part number is 1) and p6890831_111070_AIX5L_2of2.zip (Part number is 2).

6. Click **Upload**.

[Figure 24–11](#) graphically explains the steps outlined in this section, and describes how you can enter the patch details you noted in [Section 24.2.4.6.1](#) ([Figure 24–10](#)). Map the numbered items in this illustration with the numbered items in [Figure 24–10](#).

Figure 24–11 Entering Patch Details and Uploading Patch to Software Library



24.2.5 Analyzing the Environment and Identifying Whether Your Targets Can Be Patched

Before you create a patch plan and patch your targets, Oracle recommends you to run the *Patchability Report* to analyze the environment and identify whether the targets you want to patch are suitable for a patching operation.

If they are not suitable, then you can diagnose and find out whether they are not suitable due to missing properties or unsupported configuration, and also resolve them based on the recommendations provided for those issues.

To run the patchability report, follow these steps:

1. From the **Enterprise** menu, select **Reports**, then select **Information Publisher Reports**.
2. On the Information Publisher Reports page, in the table, expand **Deployment and Configuration**, then expand **Patching Automation Reports**, and then select **EM Target Patchability Report**.

Note: If you see missing property-related errors, then resolve the errors with workarounds described in [Section 24.2.5.1](#). If you see unsupported configuration-related errors, then resolve the errors with workarounds described in [Section 24.2.5.2](#).

24.2.5.1 Workarounds for Missing Property Errors

[Table 24–4](#) describes the possible missing property errors and the workarounds you can try to resolve them.

Table 24–4 *Missing Properties Error and Workarounds*

Problem	Workaround
Empty target property version	The target is not properly configured or maybe the target is unavailable. Reconfigure the target or check for metric collection errors.

Table 24–4 (Cont.) Missing Properties Error and Workarounds

Problem	Workaround
Inadequate or incomplete target information collected by Oracle Management Agent.	<p>To resolve this issue, recompute the dynamic properties and refresh the host configuration so that the Management Repository is updated with the latest configuration of the host. To do so, follow these steps:</p> <ol style="list-style-type: none"> <li data-bbox="764 384 1409 667"> <p>To recompute the dynamic properties, do one of the following:</p> <p>Option A: Stop and restart the Management Agent. This option is simpler because you do not have to understand the target model.</p> <pre data-bbox="813 541 1040 604">\$ emctl stop agent \$ emctl start agent</pre> <p>For a cluster, restart the Management Agent on all the nodes of the cluster.</p> <p>Option B: Reload the dynamic properties. This option is better because you have no blackout or downtime for monitoring.</p> <pre data-bbox="813 779 1279 800">\$ emctl reload agent dynamicproperties</pre> <p>For a specific target, run the following command:</p> <pre data-bbox="813 863 1398 905">\$ emctl reload agent dynamicproperties [<Target_name>:<Target_Type>]</pre> <p>For example:</p> <pre data-bbox="813 968 1425 1251">\$ emctl reload agent dynamicproperties oradb:oracle_database \$ emctl reload agent dynamic properties racdb_ 1:rac_database \$ emctl reload agent dynamicproperties crs:cluster \$ emctl reload agent dynamic properties wls:weblogic_j2eeserver \$ emctl reload agent dynamicproperties server1.xyz.com:host</pre> <li data-bbox="764 1272 1442 1423"> <p>To update the Management Repository with the latest configuration information, from the Enterprise menu, select Configuration, and then select Refresh Host Configuration. On the Refresh Host Configuration page, select the hosts for which the configuration must be updated, and click Refresh Hosts.</p>
Targets are not properly discovered because of inadequate or incomplete target information collected during discovery.	<p>To resolve this issue, rediscover the domain so that all the targets in the domain are discovered effectively. To do so, follow these steps:</p> <ol style="list-style-type: none"> <li data-bbox="764 1539 1360 1591"> <p>Log in to the Domain Home page using appropriate credentials. For example, Farm01_base_domain.</p> <li data-bbox="764 1608 1442 1738"> <p>On the (Farm01_base_domain) home page, from the Farm menu, select Refresh WebLogic Domain, and click Ok on all the following pages to complete the process. After successful completion of the process the domain home page is refreshed to discover all the targets afresh.</p>

24.2.5.2 Workarounds for Unsupported Configuration Errors

Table 24–5 describes the possible unsupported configuration errors and the workarounds you can try to resolve them.

Table 24–5 Workarounds for Unsupported Configuration Errors

Problem	Workarounds
Oracle RAC Instance does not have an associated Oracle RAC Database	Rediscover the Oracle RAC target and add the Oracle RAC instance to the Oracle RAC database.
The database is not mediated by the OMS	The target discovery is not appropriate. Remove the target from Cloud Control, and rediscover on all the Management Agents in the cluster.

24.3 Identifying Patches to Be Applied

This section describes how you can identify the patches to be applied.



This section is mainly for Patch Designers who want to keep track of the various patch releases, look for recommendations from Oracle, and identify the ones they want to roll out in the environment.

This section covers the following:

- [\(Online\) Using Patch Recommendations](#)
- [\(Online\) Using Knowledge Articles](#)
- [\(Online\) Using Service Requests](#)
- [\(Online\) Searching Patches on My Oracle Support](#)
- [\(Offline\) Searching Patches in Oracle Software Library](#)

24.3.1 (Online) Using Patch Recommendations

Patch recommendations are proactive notifications of potential system issues and recommendations that help you improve system performance and avert outages.

The Patch Recommendations region provides a portal to all recommended patches. From the bar graph, you can drill down to a list of recommended patch, view details about those patches, download the patches, or add them to a Patch Plan. A bar graph summarizes the number of issues found (one issue = one recommendation for one target).

Patches mentioned in the Patch Recommendation section are a collection of patches offered within MOS which can be applied as a group to one or more targets. To keep the Patch Recommendation section updated with the latest patches for your environment, there is a step called the Config Collection step that runs as a part of the patch plan when a patching job is submitted. Essentially, Config collection enables to collect the changes that happen due to application of a patch or a rollback. These updates are communicated to the OMS through the Management Agents, which ultimately help in updating the patch recommendation region.

Note: Starting with Enterprise Manager 12c, the Config Collection that is triggered at the end of patch application happens asynchronously, which means that collection may not complete when the plan completes execution. In such cases, you might need to recalculate the patch recommendations for your enterprise. Also, if the target collection has not happened properly, then too you might have to recalculate the patch recommendations.

To do so, follow these steps:

1. Run the following EM CLI commands to get the target information of a patch plan:

```
emcli get_patch_plan_data -name=<name of the plan>
```

2. Perform the following steps to determine the time when the plan was deployed on the targets:

- a. From **Enterprise** menu, select **Provisioning and Patching**, and then click **Patches and Updates**.
- b. On the Patches and Updates page, from the Plans section, select the patch plan.
- c. From the Create Plan Wizard, select **Review and Deploy**.
- d. Click the link to the track the details of the deployment.
- e. Note down the start time of the job from the Job UI page.

3. On the Config Management side, use the following attributes to calculate the collection time stamp using MGMT\$ECM_CURRENT_SNAPSHOTS view as follows:

```
start_timestamp - timestamp of the collection (in target
timezone)
last_upload_timestamp (in DB timezone) when a collection was
processed for this snapshot type.
```

A combination of the start timestamp and last uploaded timestamp attributes help you determine when the collection has happened, and thereby lets you determine if the information available in the patch recommendation region is up-to-date.

The Recommended Patches region appears by default on the Patch & Updates page. You can edit this region to filter its contents.

To view details of a recommended patch, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Patch Recommendations region, click on the bar graph pertaining to the desired patches.

Note: If you do not see the Patch Recommendations region, click **Customize Page** from the top-right corner, and then drag the Patch Recommendations region to the page.

Alternatively, click **All Recommendations** to display all recommendations in the Patch Recommendation page. The Patch Recommendation page displays all the recommendations currently available for the Cloud Control targets.

3. On the Patch Recommendations page, select a recommended patch to view the context menu appears. From the context menu, click **Full Screen**.

24.3.2 (Online) Using Knowledge Articles

Knowledge articles are documents published on My Oracle Support. These articles can either be announcements or workarounds to known issues.

Some of the knowledge articles that describe workarounds to known issues have patch numbers mentioned. You can choose to make a note of this patch number and search it on My Oracle Support or Oracle Software Library as described in [Section 24.3.4](#) or [Section 24.3.5](#), respectively.

Alternatively, you can click the patch number in the knowledge article. This takes you to the Patch Search page. On the Patch Search page, from the context menu of the patch, click **Add to Plan**, and select either **Add to New** if you want to add the patch to a new patch plan, or **Add to Existing** if you want to add the patch to an existing patch plan.

24.3.3 (Online) Using Service Requests

Service requests are support requests raised on My Oracle Support to report and track issues, and receive online assistance from Oracle in resolving those issues.

Some of the service requests that describe workarounds to known issues have patch numbers mentioned. You can choose to make a note of this patch number and search it on My Oracle Support or Oracle Software Library as described in [Section 24.3.4](#) or [Section 24.3.5](#), respectively.

Alternatively, you can click the patch number in the knowledge article. This takes you to the Patch Search page. On the Patch Search page, from the context menu of the patch, click **Add to Plan**, and select either **Add to New** if you want to add the patch to a new patch plan, or **Add to Existing** if you want to add the patch to an existing patch plan.

24.3.4 (Online) Searching Patches on My Oracle Support

If you already know about the existence of a patch from external sources such as blogs, Oracle technology forums, or from colleagues, then use the search functionality to search for those patches. The search functionality enables you to perform more flexible and advanced searches, and offers capabilities such as saving a search that is used routinely, and searching based on existing saved searches. All of this lets you perform searches more quickly and efficiently.

To search a patch on My Oracle Support, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.

2. On the Patches & Updates page, in the Patch Search region, enter the search parameters you want to use and click **Search**.

Note: If you do not see the Patch Search region, click **Customize Page** from the top-right corner, and then drag the Patch Search region to the page.

Alternatively, you can use the **Saved** tab to search any previously save searches. You can also use the **Recent** tab to access any recently performed identical (or similar) search.

Once the patch search is complete, the results appear in the **Patch Search Results** page. On this page, you can select a patch and download it either to the local host (desktop) or to the Software Library.

Note: To understand the other ways of searching patches on My Oracle Support, see *My Oracle Support Help*.

24.3.5 (Offline) Searching Patches in Oracle Software Library

By default, when you search a patch on the Patches & Updates screen, the Cloud Control connects to My Oracle Support using the Internet connectivity available on that host, and searches the requested patch in My Oracle Support. This is because the search functionality is set to perform in online mode by default.

However, if your host does not have Internet connectivity, then you must switch over to offline mode so that the search can be performed in Oracle Software Library (Software Library).

To switch over to offline mode, follow these steps:

1. From the **Setup** menu, select **Proxy Settings**.
2. On the Proxy Settings page, click the **Online and Offline Settings** tab.
3. In the Online and Offline Settings tab, in the Settings section, select **Offline**.

Note: In offline mode, you cannot:

- Search and download patches from My Oracle Support
 - Resolve patch conflicts with merge patches
 - View the Related Activity region
 - Access Quicklinks
 - View or create upgrade plans
-
-

To search a patch in the Software Library, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Patch Search region, enter the search parameters you want to use and click **Search**.

Note: If you do not see the Patch Search region, click **Customize Page** from the top-right corner, and then drag the Patch Search region to the page.

Once the patch search is complete, the results appear in the **Patch Search Results** page.

24.4 Applying Patches

This section describes how you can create a patch plan with patches, save the patch plan as a patch template, create a new patch plan out of that template, and then apply the patches.

This section covers the following:

- [Creating a Patch Plan](#)
- [Accessing the Patch Plan](#)
- [Analyzing, Preparing, and Deploying Patch Plans](#)
- [Switching Back to the Original Oracle Home After Deploying a Patch Plan](#)
- [Saving Successfully Analyzed or Deployed Patch Plan As a Patch Template](#)
- [\(Optional\) Creating a Patch Plan from a Patch Template and Applying Patches](#)
- [Patching Oracle Exadata](#)

Note: To be able to access the SQL application functionality as a part of SOA Infrastructure patching, you must ensure that you apply the patch no XYZ before creating a SOA patch plan.

24.4.1 Creating a Patch Plan



This section is mainly for Patch Designers who want to create patch plans.

To create a patch plan, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, identify the patches you want to apply as described in [Section 24.3](#).
3. On the Patch Recommendations page or on the Patch Search page (depending on how you identified the patch), select a patch you want to add to the Patch Plan.
4. From the context menu, click **Add to Plan**, and select **Add to New**.

Note: If you have already created a patch plan, and if you want to add patches to that patch plan, then you can select **Add to Existing**.

5. In the Create a New Plan window, enter a unique name for your Patch Plan, and click **Create Plan**.

The patch you select and the target it is associated with get added to the plan.

Note:

- If the patch you selected impacts other targets, then you are prompted to add the impacted targets as well.
 - When you create a Patch Plan, you can add a target that is a member of any system target in Cloud Control. When doing so, the other member targets of that system are automatically added to the Patch Plan. A system is a set of infrastructure components (hosts, databases, application servers, and so on) that work together to host your applications. In Cloud Control, a system and each of the components within it are modeled as individual target types that can be monitored.
 - For Oracle WebLogic Server, using a single patch plan, you can patch only one domain. However, if it is a shared domain, then the Administration Servers and Managed Servers running on different domains, which are shared with the domain being patched, are automatically added into the same plan.
 - For Oracle SOA Infrastructure targets, all the SOA WebLogic domains that must be shutdown to patch the SOA targets are added to the patch plan as impacted targets. Therefore, the Administration Server and the Managed Servers running in each of these domains also are affected, and form the *Other impacted targets* when creating a patch plan.
-
-

24.4.2 Accessing the Patch Plan



This section is mainly for Patch Designers who want to access the patch plans they have created.

To access the patch plan you created in [Section 24.4.1](#), use one of the following approaches.

Approach 1: Accessing Patch Plan from Plans Region

To access the patch plan from the Plans region, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.

2. On the Patches & Updates page, in the Plans region, click the Patch Plan you want to view. Alternatively, select the Patch Plan, and in the context menu, click **View**. The Create Plan Wizard appears.

To filter the plans table, select **All Plan Types** or **Patch** depending on your preference. To search for a plan, enter a plan name or partial plan name in the search box, then click the search button.

Note:

- If you do not see the Plans region, click **Customize Page** from the top-right corner, and then drag the Plans region to the page.
 - To view only the plans that you created, click the icon of a person in the Plans region.
-
-

Approach 2: Accessing a Patch Plan from the Patch Recommendations Region

To access the patch plan from the Patch Recommendations region, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Patch Recommendations region, click **All Recommendations**.

Note: If you do not see the Patch Recommendations region, click **Customize Page** from the top-right corner, and then drag the Patch Recommendations region to the page.

3. On the Patch Recommendations page, in the table, a patch that is already part of a plan is shown with the plan icon in the **In Plan** column. Click the icon to display all plans with which the patch is associated, and then click a plan to open the Create Plan Wizard.

24.4.3 Analyzing, Preparing, and Deploying Patch Plans



This section is mainly for Patch Designers who want to analyze the patch plans and deploy them to roll out the patches.

To analyze the patch plan you created in [Section 24.4.1](#) and deploy it (or save it as a patch template), follow these steps:

1. Access the patch plan using one of the approaches described in [Section 24.4.2](#). Cloud Control displays the Create Plan Wizard.
2. On the Plan Information page, do the following:
 - a. In the Overview section, validate the Patch Plan name. You can choose to edit it if you want.

- b. (Optional) Select a date and time when you want to deploy the Patch Plan, and enter a short description to describe the Patch Plan.
- c. (Optional) Add administrators or roles who should have access to the Patch Plan by clicking **Add**.

In the Add Privileges to Administrators window, select an administrator or role, the permission you want to grant, and then, click **Add Permission**.

Note:

- You can only add administrators or roles that you previously created in Cloud Control. You cannot create them from within a Patch Plan. For information on roles and privileges required for patch plan and patch templates, see [Section 24.2.2](#).
 - To remove an administrator or role, select the administrator or role, and from the context menu, click **Remove**.
-
-

- d. Click **Next**.
3. On the Patches page, do the following:
 - a. Review the patches added to the Patch Plan. Any recommended patches for your configuration are automatically added to the Patch Plan. In addition, any patches that you added manually are listed.

To associate additional targets to a patch that is already in your Patch Plan, follow the instructions outlined in [Section 24.6.8](#).

To view details of a patch, select the patch, and from its context menu, click **View**. To temporarily remove the patch from analysis and deployment, click **Suppress**. This leaves the patch in the Patch Plan, but does not consider it for analysis and deployment.

- b. Click **Next**.
4. On the Deployment Options page, do the following:

- a. In the Where to Stage section, select one of the following options:

Yes, if you want the wizard to stage the patches from the Software Library to a temporary location accessible to the target host, before the patch is applied on the target. By default, the wizard stages the patches to a default location on the target host, but if you want to change the location, you can enter a location where the patch can be staged.

No, if you have already manually staged the patches to a temporary location accessible to the target host. This can even be a shared, NFS-mounted location. In this case, ensure that you download the patch you want to apply. Go to the location (parent directory) where you want to stage the patch, create a subdirectory with the same name as the patch ZIP file, extract the contents of the patch ZIP file in this subdirectory. Then, enter the absolute path to the parent directory where you have manually staged the patches.

For example, if downloaded patch 699099.zip, and if the stage location, which is the parent directory, is `/u01/app/oracle/em/stagepatch`, then in this parent directory, create a subdirectory titled 699099 and extract the contents in it. Then, enter `/u01/app/oracle/em/stagepatch` as the stage path.

For tips for entering a stage location, click the question mark icon against the **Stage Location** list.

- b. In the How to Patch section, select one of the following:

For standalone databases targets and Oracle Grid Infrastructure targets that are part of Oracle Exadata, you have a choice between in-place patching and out-of-place patching, so select the one that suits your requirement:

In Place, if you want to directly patch the existing original Oracle home of the target without cloning the original Oracle home.

Out of Place, if you want to clone the existing Oracle home of the database and patch the cloned Oracle home instead of the original Oracle home.

For Oracle RAC database, Oracle Clusterware, Oracle Grid Infrastructure, Oracle WebLogic Server, Oracle Fusion Application, and Oracle SOA Infrastructure targets the default and the only patching mechanism offered is in-place patching.

If you select in-place patching, then select one of the following modes:

Rolling, if you want to patch one node at a time. This option is applicable only to Oracle RAC databases. It is the default option and it involves very little downtime.

Parallel, if you want to patch all nodes simultaneously. This option is applicable only to Oracle RAC databases. It involves downtime because your entire system is shut down for a specified period.

- c. *(Appears only for standalone database targets and Oracle Grid Infrastructure targets that are part of Oracle Exadata)* In the What to Patch section, do the following:

If you have selected in-place patching, then review the details of the Oracle homes that will be patched. By default, all of the database instances are migrated.

If you have selected out-of-place patching, then click **Create New Location** against the Oracle home you want to clone, and enter the path to a location that is empty and has write permission. You can clone the Oracle home to any directory on the host where the target is being patched. After providing a location, if you want to change it, click **Edit**.

For standalone database targets, you have the option of migrating either all or only some of the database instances created from the specified Oracle home, so select the ones you want to migrate. However, for Oracle Grid Infrastructure targets that are part of Oracle Exadata, by default, all of the database instances are migrated.

Note: After the cloned Oracle home is patched, and after the database instances are migrated to the cloned Oracle home, you can choose to retain the original Oracle home or delete it if there are no other targets running from that Oracle home.

- d. (Optional) In the Customization section, to customize the default deployment procedure used by the Patch Plan, click **Create Like and Edit**. To use a customized deployment procedure, select the customized procedure from the list.

Note: After you save a customized deployment procedure, you will be taken to the deployment procedure Manager page. To use the customized deployment procedure, you must return to the Deployment Options page of the Create Plan Wizard.

(Appears only for Oracle WebLogic and Oracle SOA Infrastructure targets) If you are patching an Oracle WebLogic Server target or Oracle SOA Infrastructure targets, you can set a timeout value after which the server is forcefully shut down if it was not shut down by default. By default, the shutdown time is 30 minutes, but if you want to change the value, you can enter a value in the **Timeout for Shutdown (in minutes)** field.

Oracle recommends that you set a timeout value, and ensure that it is based on monitoring of real time systems.

(Appears only for SOA Infrastructure targets) If the SOA Infrastructure patch you are applying involves SQL application functionality, then you must provide the absolute path to the SQL scripts in the **Post-Install SQL Script Metadata** field. For information about the SQL script location, refer to the readme document for the respective patch.

Note: To patch SOA Infrastructure targets running on a Windows host, you must ensure that you use the environmental variable `%FMW_ORACLE_HOME%` as displayed in the following graphic to provide a relative path to the SQL files in the SOA patch. Providing an absolute path or using the environmental variable `%ORACLE_HOME%` will result in an error.



Post-Install SQL Script Metadata * Format is patch1:sql_script1,sql_script2;patch2:sql_script3;...
 Provide the data for post-installation SQL script application to metadata repository.

Note: Ensure that the SQL scripts that you may need to provide as a part of patching SOA Infrastructure targets are JDBC-compliant, if not, the patch plan will fail during the analysis phase.

To perform SOA Infrastructure patching on a Windows operating system, you must ensure that you shutdown all the servers running from the SOA instance home being patched. Stopping just the SOA servers running out of the SOA instance home will result in an error.

- e. Roll back functionality is supported on the following targets: Management Agent, Oracle WebLogic Server, and Oracle SOA Infrastructure.

In the Rollback section, select **Plan deployment rolls back the patches in the plan** to rollback the patches listed in the plan rather than deploy them. For instructions on rolling back a patch, see [Section 24.6.13](#).

Rollback

Plan deployment **rolls back** the patches in this plan 

Note: For Oracle WebLogic Server targets, patching and rollback happens at domain level. When Oracle WebLogic Server targets are selected for rollback, the domain along with the Administration Server and the Managed Servers are rolled back. You cannot select the instances you want to rollback, and deselect the ones you do not want to rollback from the domain.

Note: For SOA Infrastructure targets, patching and rollback happens at instance home level, which means, you can select the SOA Oracle home instances that you want to patch or from where you want to rollback the existing patches. If there are other servers running from the SOA home being rolled back, then all of these servers and their corresponding domains will also be rolled back along with the SQL metadata scripts that can be rolled back. Some of the SQL metadata scripts cannot be rolled back, in which case, Cloud Control will rollback the patch (bits in the Oracle Home) but the SQL remains unchanged.

While patching a SOA setup, if the patch application fails on one of the Managed Servers, and succeeds on other Managed Servers, there will **not** be an automatic rollback operation to remove the patch from all Managed Servers where the patch was successfully applied. However, you will be notified about the failure, so you can manually rollback the patch.

Typically, you will rollback a patch for the following reasons:

- If you had forcefully applied an incoming patch that conflicted with a patch in the Oracle home, and now you want to uninstall that applied patch.
- If the applied patch does not meet your requirements satisfactorily; the patch might have fixed a bug, but at the same time, introduced other bugs in the process.

- f. In the Credentials section, select the credentials.

For patching Oracle WebLogic Server targets and Oracle SOA Infrastructure targets, you need the following sets of credentials:

- **Oracle WebLogic Domain Administrator Credentials:** These credentials are required to connect to the admin server of the domain which monitors all the Managed Servers present in that domain.

- **Oracle WebLogic Server Home Credentials:** These credentials are required to connect to all the Oracle homes present on different hosts.

You can also choose to override the existinf credentials by selecting **Override Preferred WebLogic Domain Administrator Credentials** and **Override Preferred WebLogic Home Credentials**. However, if you choose to override the preferred credentials, then you must validate the credentials. For Oracle WebLogic Server targets, you can validate only the Oracle WebLogic Server Home credentials, and not the administrator credentials.

Note: The validation of credentials fails when the Management Agent is down, or when the credentials are incorrect.

- g. Click **Next**.
5. On the Validation page, click **Analyze** to check for conflicts. For information about what checks are performed in the validation screen, see [Section 24.1.3.3](#).

Upon validation, if there are conflicts between the two patches, then you might be recommended to request for replacement patches. In this case, click **Request Replacement Patches**.

If there is a Merge Patch already available, you can directly opt to replace the conflicting patches with the Merge Patch. In this case, click **Replace Conflicting Patches**.

Click **Next**.

6. On the Review & Deploy page, review the details and do one of the following:
- If you are patching standalone databases in out-of-place patching mode [that is, if you have selected **Out of Place** in Step (4 b)], then click **Prepare**. This essentially clones the source Oracle home and patches it. While this happens, the source Oracle home and their database instances are up and running.

After the prepare operation ends successfully, click **Deploy**. This essentially switches the database instances from the source Oracle home to the cloned and patched Oracle home. The prepare and deploy operation enable you to minimize the downtime.
 - If you are patching any other target in any other mode, click **Deploy**.

Note: To save a successfully analyzed or deployed patch plan as a patch template, see [Section 24.4.5](#).

24.4.4 Switching Back to the Original Oracle Home After Deploying a Patch Plan

If you had patched an Oracle Grid Infrastructure target, which was part of Oracle Exadata, in out-of-place patching mode, and if you now want to switch back to the original home for some reason, then you can use the *Switchback* option available in the Create Plan Wizard. The advantage of using this option is, you do not actually roll back the patches from the cloned and patched Oracle home; you only switch back to the old, original Oracle home that exists without the patches.

Note:

- The *Switchback* option is available only for Oracle Grid Infrastructure targets, which are part of Oracle Exadata, and only when they are patched in out-of-place patching mode.
 - You can switch back only if you have successfully analyzed and deployed a patch plan.
-

To switch back to the original Oracle home after a patch plan is deployed, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Plans region, click the successfully analyzed and deployed patch plan you used for patching Oracle Grid

Infrastructure targets. Alternatively, select the patch plan, and in the context menu, click **View**. The Create Plan Wizard appears

3. In the Create Plan Wizard, on the Review & Deploy page, click **Switchback**.

24.4.5 Saving Successfully Analyzed or Deployed Patch Plan As a Patch Template



This section is mainly for Patch Designers who want to save the successfully analyzed or deployed patch plans as patch templates so that operators can consume them to create fresh patch plans with the approved patches and predefined deployment options.

To save a patch plan as a patch template, follow Step (1) to Step (5) as outlined in [Section 24.4.3](#), and then for Step (6), on the Review & Deploy page, click **Save as Template**. In the Create New Plan Template dialog, enter a unique name for the patch template, and click **Create Template**.



Oracle recommends you to follow this as a best practice if you have to roll out in a mass scale over a period of time involving more administrators. If you have a large data center, then as a Patch Designer, create a patch plan and apply the patches on a few databases, test if the patches are being applied successfully, then save the plan as a template. Later, have your Patch Operators create patch plans out of these templates so that they can roll out the same set of patches to the rest of the databases in the data center.

24.4.6 (Optional) Creating a Patch Plan from a Patch Template and Applying Patches

Once a successfully analyzed or deployed patch plan is saved as a patch template, you can create patch plans out of the template, associate targets you want to patch, and deploy the newly created patch plan.

This is purely an optional step. You do not have to save your patch plans as patch templates to roll out patches. You can roll out patches directly from a patch plan as described in [Section 24.4.3](#).



This section is mainly for Patch Operators who want to create patch plans from patch templates for rolling out the patches.

To create patch plans out of the patch templates, use one of the following approaches:

Approach 1

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Plans region, select the patch template you want to use to create a patch plan out of it.

3. From the context menu, select **Create Plan**.
4. In the Create Plan from Template dialog, enter a unique name for the patch plan, select the targets on which you want to patch, and click **Create Plan**.
5. Return to the Patches & Updates page, and in the Plans region, click the patch plan you want to use. Alternatively, select the patch plan, and in the context menu, click **View**. The Create Plan Wizard appears.
6. In the Create Plan Wizard, go to the Validation page, and click **Re-Analyze** to analyze the patch plan with the newly associated targets.
7. After successfully analyzing the patch plan, on the Validation page, click **Next**.
8. On the Review & Deploy page, click **Deploy**.

Approach 2

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Plans region, do one of the following:
 - Select a patch template. From the context menu, select **View**. The Edit Template Wizard appears.
 - Click the name of a patch template. The Edit Template Wizard appears.
3. In the Edit Template Wizard, click **Create Plan**.
4. In the Create Plan from Template dialog, enter a unique name for the patch plan, select the targets on which you want to patch, and click **Create Plan**.
5. Return to the Patches & Updates page, and in the Plans region, click the patch plan you want to use. Alternatively, select the patch plan, and in the context menu, click **View**. The Create Plan Wizard appears.
6. In the Create Plan Wizard, go to the Validation page, and click **Re-Analyze** to analyze the patch plan with the newly associated targets.
7. After successfully analyzing the patch plan, on the Validation page, click **Next**.
8. On the Review & Deploy page, click **Deploy**.

24.4.7 Patching Oracle Exadata

Using patch plans, you can patch the Oracle RAC database targets and the Oracle Grid Infrastructure targets (Oracle Clusterware) running on an Exadata Database Machine.

Exadata Patching can be performed in two modes: In Place Patching, and Out-of-place Patching, though Oracle recommends you to use the Out-of-place patching mechanism as the downtime involved is much lesser. For more information about Exadata Out Of Place Patching, see [Section 24.4.7.1](#).

For information about the supported Exadata releases, see [Section 24.1.5](#).

However, note that patch plans do not patch the Exadata Database Machine's compute node entities such as the operating system and firmware, and also its storage cells. They patch only the associated Oracle RAC database targets and the Oracle Grid Infrastructure (Oracle Clusterware) targets running on the machine.

Note: Oracle Exadata Database Machine recommended bundle patches that apply to Oracle RAC and the Oracle Grid Infrastructure targets (Oracle Clusterware) are tested and certified with Cloud Control.

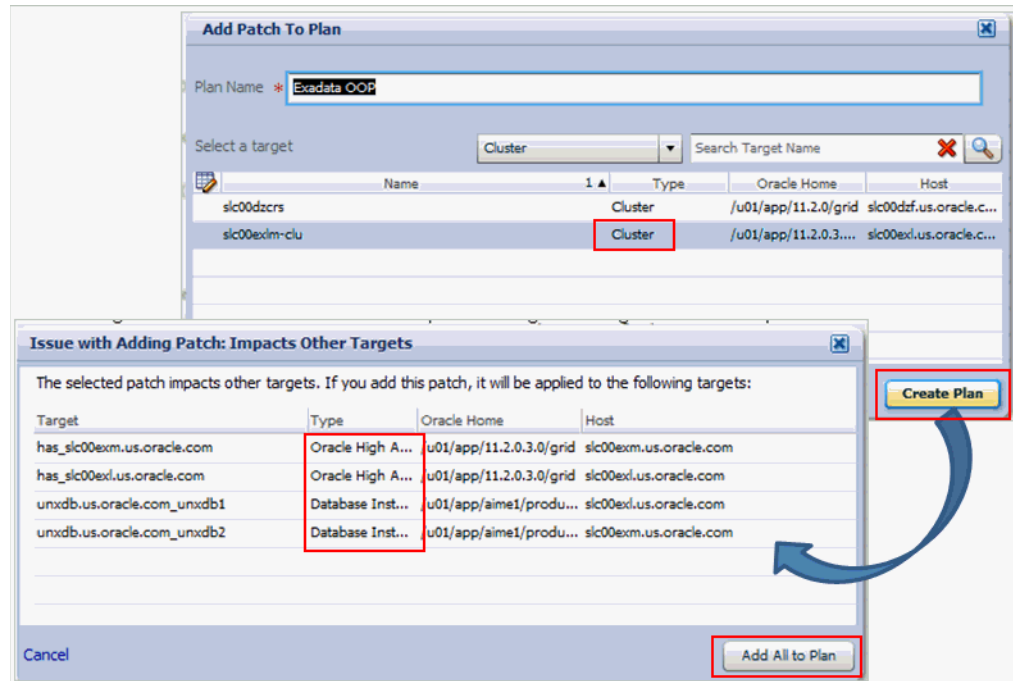
Therefore, when you create a patch plan with an Exadata Database Machine recommended bundle patch, make sure you add the cluster or the Oracle RAC database target running on the Exadata Database machine. The patch plan automatically recognizes their association with the Exadata Database machine, and prompts you to add all the impacted targets running on that machine. For example, if you select the cluster target, it prompts you to add all the Oracle RAC database targets and the Oracle Grid Infrastructure targets that are part of that cluster running on the Exadata Database Machine.

To patch an Exadata Database machine, follow these steps:

1. Identify the Exadata Database Machine recommended bundle patch you need to apply, as described in [Section 24.3](#).
2. Create a patch plan as described in [Section 24.4.1](#).
3. Add the cluster or the Oracle RAC database target running on the Exadata Database machine, and analyze and deploy the patch plan as described in [Section 24.4.3](#).

The following illustrate how you can add an Exadata Database Machine recommended bundle patch to a new patch plan, select a cluster target, and all the other associated Oracle RAC database targets and Oracle Grid Infrastructure targets.

Figure 24–12 Adding Exadata Database Machine Bundle Patch to a Patch Plan



24.4.7.1 Exadata Out-Of-Place Patching Of Oracle Grid Infrastructure and Oracle RAC Targets

Exadata Out-of-place patching mechanism allows you patch the Oracle Grid Infrastructure and Oracle RAC targets by making a copy of their existing Oracle homes, and patching the cloned Oracle homes. Once the cloned homes are patched, you can migrate the instances to run from the cloned home, which means there will be minimal downtime while switching over the instances, but not a significant downtime.

Figure 24–13 illustrates how Oracle Grid Infrastructure and Oracle RAC targets running on an Exadata Database Machine get patched in Out-of-place patching mode:

Figure 24–13 Out Of Place Patching Of Clusters



The migration of these instances can be performed in the following modes:

- **Full Migration:** If you choose to migrate all the database instances running in your data center in one session, then it is termed as Full Migration.
- **Partial Migration:** If you choose to migrate only some of the instances depending on the downtime you can afford in your data center in one session, then it is termed as Partial Migration. However, you must ensure that you migrate the remaining instances in the following sessions. This approach is particularly useful when you have multiple instances running out of an Oracle home.

Note: for steps on how to perform Full Migration or Partial Migration of Oracle Grid Infrastructure Targets and Oracle RAC Targets running on Exadata Database Machine, see [Section 24.4.3](#).

Switch Back is an option available exclusively for Oracle Grid Infrastructure targets and Oracle RAC targets running on Exadata machine, that enables you to switch the instances from the newly cloned Oracle homes back to the original Oracle homes in case of any problems.

For more information on how to perform a Switch Back, see [Section 24.4.4](#).

24.5 Diagnosing and Resolving Patching Issues

This section describes the following:

- [Diagnosing Patching Issues](#)
- [Resolving Patching Issues](#)
- [Rolling Back Patches](#)

24.5.1 Diagnosing Patching Issues

While analyzing or deploying patch plans, you might see errors if the following are true:

- If the OMS or the Management Agent is down
- If the Software Library is not properly configured
- If there is no connectivity to My Oracle Support (in online mode)
- If there is no Management Repository
- If there are no collections
- If there are host or Oracle home security issues
- If there are inherent OPatch or SQL errors
- If the patch plan consists of *non-homogenous* patches, for example, a combination of one-off patches and patch sets
- (For Oracle WebLogic Targets only) If there are inherent problems with the SmartUpdate tool.
- (For Oracle WebLogic Targets only) If there is problem discovering Oracle WebLogic targets reporting to the OMS.

You will see these errors in the following places:

- In the header section of the Validation page or the Review page in the Create Plan Wizard ([Figure 24–14](#))
- In the Issues to Resolve section of the Validation page ([Figure 24–15](#))
- In the Plans region of the Patches & Updates page ([Figure 24–16](#)).

Figure 24–14 Patch Plan Errors Displayed on the Validation Page

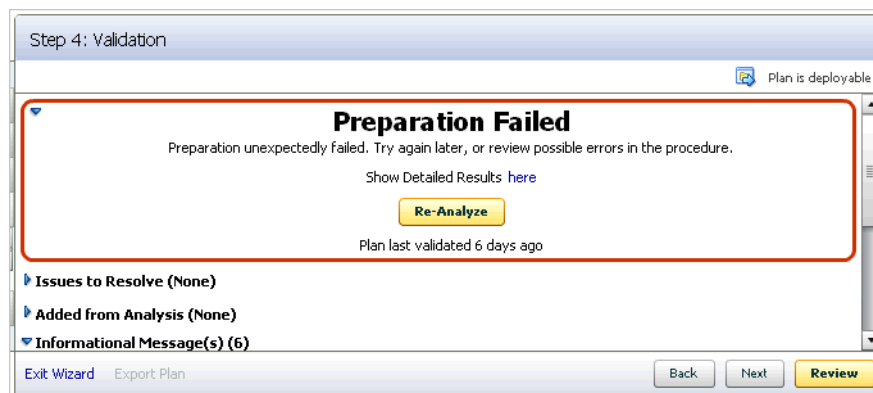


Figure 24–15 Patch Plan Errors Displayed in the Issues to Resolve Section

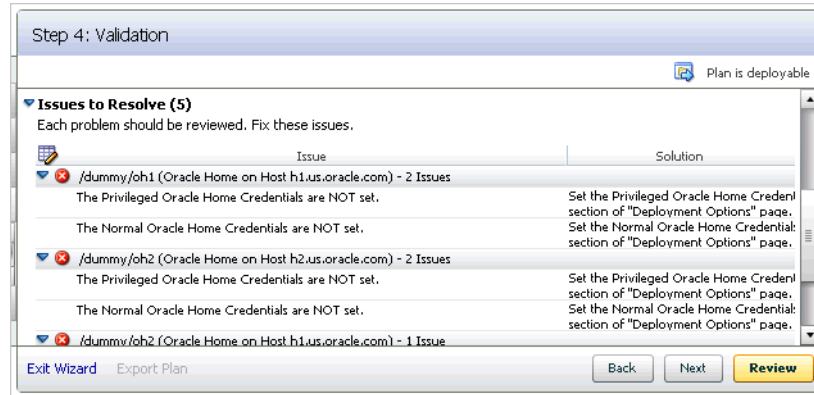
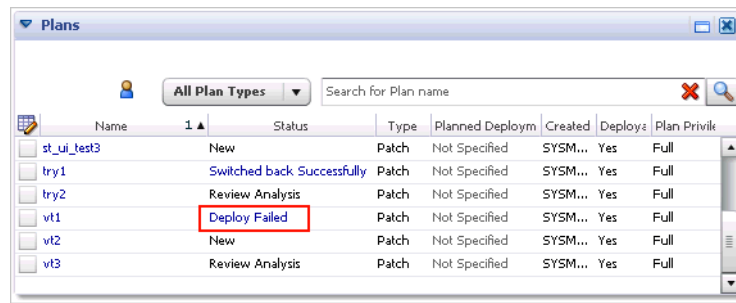


Figure 24–16 Patch Plan Errors Displayed in the Plans Region



24.5.2 Resolving Patching Issues

Table 24–6 lists the different phases that the patch plan goes through, the different states the phases can have, and how you can diagnose and resolve the errors.

Note: Also refer to the troubleshooting tips described in [Section E.2](#).

Table 24–6 Diagnosing Patching Issues

Phase	State	Diagnosis and Resolution
Analysis	Analysis In Progress	N/A
	Analysis Error	Review the following log file: <gc_inst>/sysman/log/emoms.log
	Issues Remain	In the Create Plan Wizard, on the Validation page, review the issues listed in the Issues to Resolve section. In the Issues to Resolve section, if an error message states that you must click Show Detailed Results here , then click it. On the Procedure Activity Status page, in the Status Detail table, review the status of each of the steps. Click the status to view the log details.
	Conflicts Detected	In the Create Plan Wizard, on the Validation page, review the issues listed in the Issues to Resolve section. In the Issues to Resolve section, if an error message states that you must click Show Detailed Results here , then click it. On the Procedure Activity Status page, in the Status Detail table, review the status of each of the steps. Click the status to view the log details.
Preparation	Ready for Deployment	N/A
	Preparation In Progress	N/A
	Preparation Error	Review the following log file: <gc_inst>/sysman/log/emoms.log
	Preparation Failed	On the Validation page, click Show Detailed Results here . On the Procedure Activity Status page, in the Status Detail table, review the status of each of the steps. Click the status to view the log details.
Deploy	Preparation Successful	N/A
	Deployment In Progress	N/A
	Deployment Error	Review the following log file: <gc_inst>/sysman/log/emoms.log
	Deployment Failed	On the Validation page, click Show Detailed Results here . On the Procedure Activity Status page, in the Status Detail table, review the status of each of the steps. Click the status to view the log details.
	Deployment Successful	N/A

24.5.3 Rolling Back Patches

If you want to roll back the patches, follow the rollback instructions outlined in the ReadMe that is packaged with the patch you applied.

Roll back functionality is supported on the following targets: Management Agent, Oracle WebLogic Server, and Oracle SOA Infrastructure. For more information about the steps to rollback, see [Section 24.6.13](#). For all other targets, Cloud Control does not support automatic rollback of patches, and therefore, you must roll back the patches manually.

24.6 Additional Tasks You Can Perform

This section covers the additional tasks you can perform with patch plans. In particular, it covers the following:

- [Viewing or Modifying Patch Template](#)
- [Saving a Deployed Patch Plan as a Patch Template](#)
- [Creating a Compliance Standard from a Patch Template](#)
- [Downloading Patches from Patch Template](#)
- [Deleting Patch Template](#)
- [Deleting Patch Plan](#)
- [Converting Nondeployable Patch Plan to Deployable Patch Plan](#)
- [Associating Additional Targets to a Patch in a Patch Plan](#)
- [Resolving Patch Conflicts](#)
- [Analyzing the Results of Patching Operations](#)
- [Customizing Patching Deployment Procedure](#)
- [Patching Primary and Standby Databases Configured with Oracle Data Guard](#)
- [Rolling Back Patches](#)

24.6.1 Viewing or Modifying Patch Template

To view or modify a patch template, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Plans region, do one of the following:
 - Select a patch template. From the context menu, select **View**. The Edit Template Wizard appears.
 - Click the name of a patch template. The Edit Template Wizard appears.

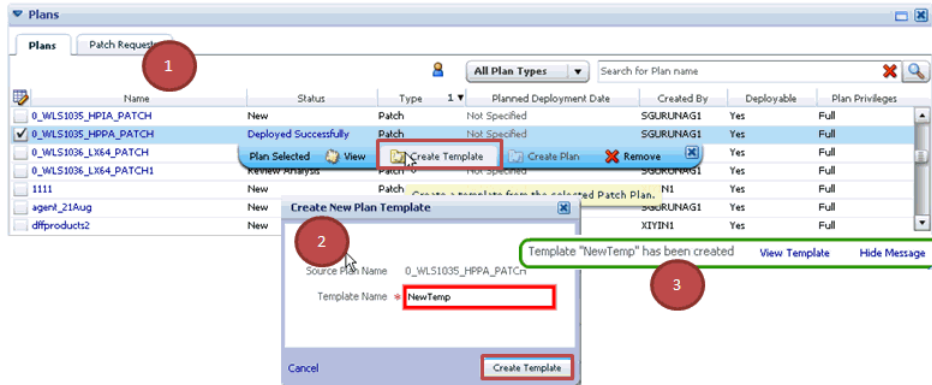
Note:

- An administrator who created the patch template and the super administrator of Cloud Control can modify a patch template.
 - You can modify only the description and the deployment date in the patch template.
-
-

24.6.2 Saving a Deployed Patch Plan as a Patch Template

If you have already analyzed and deploy a patch plan, and if you want to save that patch plan as a patch template, then use one of the following approaches:

Approach 1



1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Plans region select a successfully analyzed deployable Patch Plan. The context menu appears.

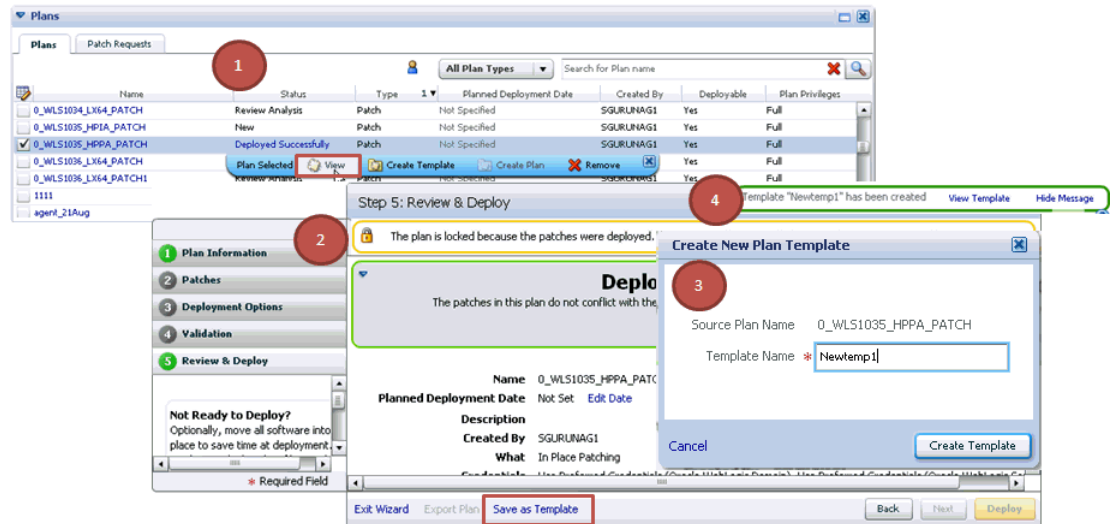
Note: You can create a patch template only from one Patch Plan at a time.

3. From the context menu, select **Create Template**. The Create New Plan Template dialog appears.
4. Enter a unique name for the template, then click **Create Template**.

Note: When you select a plan, the **Create Template** option is not visible if you:

- Select a nondeployable Patch Plan or a deployable Patch Plan that has either not been analyzed or resulted in errors after being analyzed.
 - Do not have the privileges to view the Patch Plan that you selected.
 - Do not have the privileges to create a template.
-

Approach 2

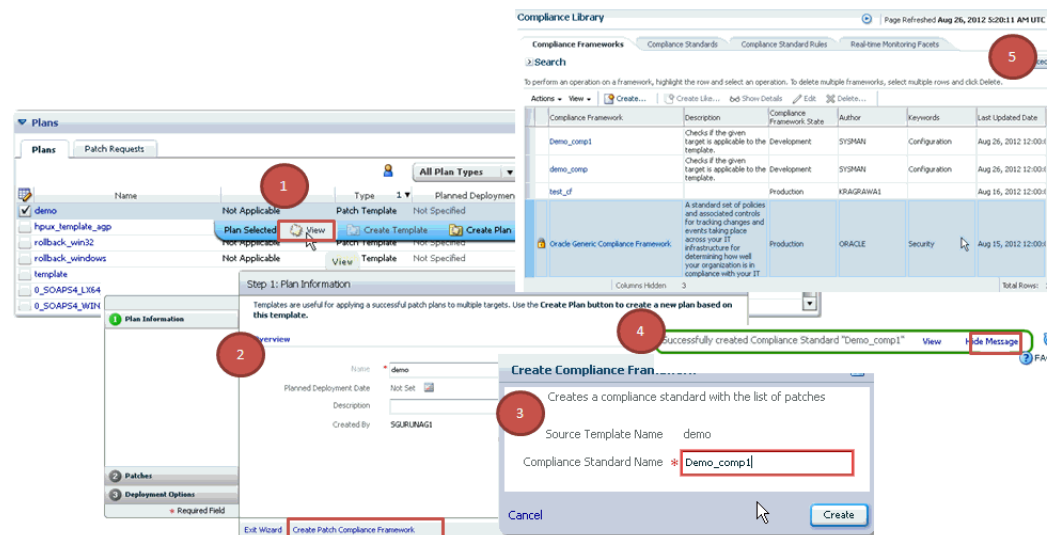


1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the **Patches & Updates** page, in the **Plans** region do one of the following:
 - Select a successfully analyzed deployable Patch Plan. From the context menu, select **View**. The **Create Plan Wizard** appears.
 - Click the name of a successfully analyzed deployable Patch Plan. The **Create Plan Wizard** appears.
3. In the **Create Plan Wizard**, in the **Review & Deploy** page, click **Save as Template**.
4. Enter a unique name for the template, then click **Create Template**.

Note: You must create patch templates only with unique names.

24.6.3 Creating a Compliance Standard from a Patch Template

To create a compliance standard from a patch template, follow these steps:



1. On the Patches & Updates page, in the Plans region select a patch plan template. The context menu appears.
2. From the context menu, select **View**. The Edit Template Wizard appears.
3. On the Plan Information page, click **Create Patch Compliance Framework**.
4. In the Create Compliance Framework dialog, enter a unique name for the compliance standard, and click **Create**.
5. A confirmation message appears when the compliance is successfully created. Click **View** to access the Compliance Library Page.

24.6.4 Downloading Patches from Patch Template

To download a patch from a patch template, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Plans region, select a patch template.
3. From the context menu, select **View**. The Edit Template Wizard appears.
4. In the Edit Template Wizard, on the Patches page, click a patch number. The patch details page appears.
5. On the patch details page, click **Download**.

24.6.5 Deleting Patch Plan

To delete a patch plan, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Plans region, click the Patch Plan you want to delete. From the context menu, click **Remove**.

Note: If you do not see the Plans region, click **Customize Page** from the top-right corner, and then drag the Plans region to the page.

24.6.6 Deleting Patch Template

To delete a patch template, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Plans region select one or more patch templates. The context menu appears.
3. From the context menu, select **Remove**.

Note: n administrator who created the patch template and the super administrator of Cloud Control can modify a patch template.

24.6.7 Converting Nondeployable Patch Plan to Deployable Patch Plan

To make a nondeployable Patch Plan deployable, divide the Patch Plan into smaller deployable plans that contain only homogenous patches and targets.

Note: For more information, see [Section E.2.6.1](#).

24.6.8 Associating Additional Targets to a Patch in a Patch Plan

To associate additional targets to a patch in a patch plan, use one of the following approaches:

Approach 1

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Plans region, select a Patch Plan to which the patch belongs. From the context menu that appears, select **View**.

Note: If you do not see the Plans region, click **Customize Page** from the top-right corner, and then drag the Plans region to the page.

3. In the Create Plan Wizard, on the Patches page, Click **Add Patch**. The Edit Search window appears.
4. In the Edit Search window, search the patch to which you want to associate additional targets.
5. Select the patch that you want to add, then click **Add to This Plan**. The Add Patch To Plan window appears.
6. In Add Patch To Plan window, search and select the additional targets that you want to associate with the patch, and then, click **Add Patch to Plan**.

Note: Ensure that you select only homogeneous targets.

For Oracle WebLogic Server, using a single patch plan, you can patch only one domain. However, if it is a shared domain, then the admin servers and Managed Servers running on different domains, which are shared with the domain being patched, are automatically added into the same plan.

Approach 2

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Patch Recommendations region, click the graph.

Note: If you do not see the Patch Recommendations region, click **Customize Page** from the top-right corner, and then drag the Patch Recommendations region to the page.

3. On the Patch Recommendations page, select a patch.
4. From the context menu, select **Add to Plan**, then **Add to Existing**, and select the plan you want to add the patch to.

The patch you selected and the target it is associated with get added to the existing plan.

Approach 3

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Patches & Updates**.
2. On the Patches & Updates page, in the Search region, search a patch you want to add to the patch plan.

Note: If you do not see the Search region, click **Customize Page** from the top-right corner, and then drag the Search region to the page.

3. On the Patch Search page, click the patch to view its details.
4. On the patch details page, click **Add to Plan**, then **Add to Existing**, and select the plan you want to add the patch to.

The patch you selected and the target it is associated with get added to the existing plan.

24.6.9 Resolving Patch Conflicts

If the patches in the patch plan conflict among themselves or with patches in the Oracle home, then you can do one of the following to resolve the conflict:

- Request for a merge patch of the conflicting patches. To do so, click **Request Patch** on the Validation page.
- Roll back the conflicting patches in the Oracle home and forcefully apply the incoming patches. To do so, on the Deployment Options page, in the Advanced Patching Options section, from the **Conflict Resolution** list, select **Forcefully apply incoming patches**.
- Skip the conflicting patches. To do so, on the Deployment Options page, in the Advanced Patching Options section, from the **Conflict Resolution** list, select **Skip conflicting patches**.

24.6.10 Analyzing the Results of Patching Operations

If you want to analyze the results of the patching operations you have done over a period of time, then run the *EM Deployable Patch Plan Execution Summary*. The report shows the number of deployable and nondeployable plans you have had in the past, and provides a breakdown of the deployable plans indicating how many succeeded and failed, how many were analyzed and deployed, and so on.

To run the EM Deployable Patch Plan Execution Summary report, follow these steps:

1. From the **Enterprise** menu, select **Reports**, then select **Information Publisher Reports**.
2. On the Information Publisher Reports page, in the table, expand **Deployment and Configuration**, then expand **Patching Automation Reports**, and then select **EM Deployable Patch Plan Execution Summary**.

24.6.11 Customizing Patching Deployment Procedure

When you submit a patch plan, the patch plan automatically selects an appropriate patching deployment procedure based on the targets you have added to the plan, and

runs it internally to patch the targets. For information about the patching deployment procedures offered by Cloud Control, see [Section 24.1.5](#). These deployment procedures are default procedures created considering the best practices in the industry to ensure that they meet all your patching requirements. However, although the default procedures are self-sufficient and can meet most of your requirements, there might be occasions when you might want to customize the procedures to include additional custom steps, disable unwanted steps, run some additional scripts before or after shutting down the instances or applying the patch, and so on to suit your requirements.

Cloud Control allows you to customize these deployment procedures - you cannot directly modify a default procedure, but you can create a copy of the default procedure and modify that to suit your requirements. Unlike other deployment procedures, you can create a copy of a default patching deployment procedure directly from the patch plan. Once you have customized a deployment procedure, you can choose to use that to patch your targets.

Note: This section describes how you can customize only the patching deployment procedures. For information about customizing deployment procedures in general, see [Chapter 33](#). The chapter explains in detail what customization means, the different ways of customizing a deployment procedure, and so on. Read the chapter if you want to learn about customizing deployment procedures.

To customize a default patching deployment procedure:

1. Go to the Deployment Options page.
2. In the Customization section, click **Create Like and Edit**.
3. Edit the deployment procedure and save it with a unique, custom name. For information about editing a deployment procedure, see [Section 33.2](#).

Note: After you save a customized deployment procedure, you will be taken to the deployment procedure Manager page. To use the customized deployment procedure, you must return to the Deployment Options page of the Create Plan Wizard.

To use a customized deployment procedure:

1. Go to the Deployment Options page.
2. In the Customization section, select the customized deployment procedure that you want to use from the list of deployment procedures.

To further customize a customized deployment procedure:

1. Go to the Deployment Options page.
2. In the Customization section, select the customized deployment procedure you want to update, then click **Customize**.

24.6.12 Patching Primary and Standby Databases Configured with Oracle Data Guard

This section covers the following:

- [Overview of Patching Primary and Standby Databases](#)

- [Patching Primary and Standby Databases](#)
- [Customizing Patching deployment procedure](#)

24.6.12.1 Overview of Patching Primary and Standby Databases

To patch the primary and standby databases that are configured with Oracle Data Guard, you can use patch plans, which inherently use the default database patching deployment procedures suitable for the targets selected in the patch plan.

The databases that act as primary or standby can be either a standalone database (single-instance) or an Oracle Real Application Cluster (Oracle RAC) database running with or without a broker.

However, the following are the limitations with patching of primary and standby databases:

- There is no support for orchestrated patching between a primary database and its standby database. Although the default database patching deployment procedures used by the patch plans automatically identify the primary and the standby databases, they do not recognize the association between them. As a result, you must manually identify the primary database and its associated standby database, and patch them separately in such a way that the standby database switches over to production mode while the primary database is being patched.
- There is no support automatically stopping and starting log shipping. You must manually stop and start the log shipping either directly or via a broker. The deployment procedures do not handle this by default. However, if you want, you can customize the deployment procedure to include additional steps that will handle this issue.
- There is no support for Oracle Data Guard in logical standby configuration.

24.6.12.2 Patching Primary and Standby Databases

To patch the primary and the standby database, follow these steps:

1. Customize the database patching deployment procedure as described in [Section 24.6.12.3](#) to include additional steps to handle stopping and starting of log shipping with or without a broker.
2. Identify the primary and standby database.
3. Patch the standby database using the customized deployment procedure in a patch plan.
4. Patch the primary database using the customized deployment procedure in a patch plan.

24.6.12.3 Customizing Patching deployment procedure

To automate the stopping and starting of log shipping, you must customize the patching deployment procedure to include two steps—one to stop the log shipping on the primary database and another to start the log shipping once the patching operation ends.

Note: You must be a *Patch Designer* to customize a deployment procedure.

To do so, follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the deployment procedure Manager page, in the Procedure Library table, select one of the following patching deployment procedure based on the target type you want to patch, and click **Create Like**.
 - *Patch Oracle Database* or *Clone and Patch Oracle Database*, for Oracle Database
 - *Patch Oracle RAC Rolling*, for the Oracle RAC Databases
3. On the Create Like Procedure page, click the **Procedure Steps** tab.
4. In the Procedure Steps tab, in the table, select **Pre-Shutdown Custom Host Command Step** and **Post-Apply SQL Custom Host Command Step**, and click **Enable**.
5. Select **Pre-Shutdown Custom Host Command Step**, and click **Edit Step**.
6. In the Edit Step Wizard, do the following:
 - a. On the Edit page, click **Next**.
 - b. On the Enter Command page, in the **Script** text box, copy the following lines, and then click **Next**.

```
# Script for Stopping Log Shipping on Primary Database, Insert before
Shutdown Database step
echo ' Executing Stop Log Shipping command on Primary Database'
PRIMDB_LIST=${target.primaryDBSIDs}
DGMGRL_CMD=${target.oraHome}/bin/dgmgrl
STATE='LOG-TRANSPORT-OFF'
if [ -z $PRIMDB_LIST ]
then
  echo " Selected Databases are not Primary Databases found. Step will be
skipped"
  exit 0
fi
PRIMDB_SPCSEP_LIST=`echo $PRIMDB_LIST | tr ',' ' '`
for EACH_PRIMDB in $PRIMDB_SPCSEP_LIST
do
  echo Running $DGMGRL_CMD on $EACH_PRIMDB
  export ORACLE_HOME=${target.oraHome}
  export ORACLE_SID=$EACH_PRIMDB
  $DGMGRL_CMD -silent / "edit database $EACH_PRIMDB SET STATE=$STATE"
  $DGMGRL_CMD -silent / "show database $EACH_PRIMDB"
done
exit 0
```

Figure 24–17 shows how the Script textbooks will look after you copy the preceding lines.

Figure 24–17 Adding a Script for Stopping the Log Shipping

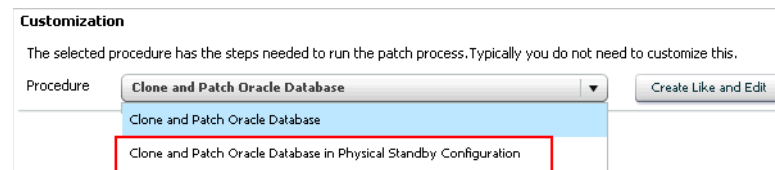
- c. On the Review page, click **Finish**.
7. In the Procedure Steps tab, in the table, select **Post-Apply SQL Custom Host Command Step**, and click **Edit Step**.
8. In the Edit Step Wizard, do the following:
 - a. On the Edit page, click **Next**.
 - b. On the Enter Command page, in the **Script** text box, copy the following lines, and then click **Next**.

```
# Script for Starting Log Shipping on Primary Database, Insert after Apply
Post SQL step
echo ' Executing Start Log Shipping command on Primary Database'
PRIMDB_LIST=${target.primaryDBSIDs}
DGMGRL_CMD=${target.oraHome}/bin/dgmgrl
STATE= ' ONLINE '
if [ -z $PRIMDB_LIST ]
then
echo " Selected Databases are not Primary Databases found. Step will be
skipped "
exit 0
fi
PRIMDB_SPCSEP_LIST=`echo $PRIMDB_LIST | tr ',' ' '`
for EACH_PRIMDB in $PRIMDB_SPCSEP_LIST
do
echo Running $DGMGRL_CMD on $EACH_PRIMDB
export ORACLE_HOME=${target.oraHome}
export ORACLE_SID=$EACH_PRIMDB
$DGMGRL_CMD -silent / "edit database $EACH_PRIMDB SET STATE=$STATE"
$DGMGRL_CMD -silent / "show database $EACH_PRIMDB"
done
exit 0
```

Figure 24–17 shows how the Script text box will look after you copy the preceding lines.

Figure 24–18 Adding a Script for Starting the Log Shipping

- c. On the Review page, click **Finish**.
9. Save the customized deployment procedure with a unique name. For example, *Clone and Patch Oracle Database in Physical Standby Configuration*.
10. While creating a patch plan as described in [Section 24.4.3](#) for patching the primary and the standby databases, in the Create Plan Wizard, on the Deployment Options page ([Chapter 24–19](#)), in the Customization section, select the customized procedure from the list.

Figure 24–19 Selecting Customized deployment procedure While Creating a Patch Plan

Note: You can customize the deployment procedure even further if you want. For more information on customizing deployment procedures, refer to [Chapter 33](#).

24.6.13 Rolling Back Patches

Roll back functionality is supported on the following targets: Management Agent, Oracle WebLogic Server, and Oracle SOA Infrastructure. To rollback patches, you must create a new patch plan, select the relevant patches to rollback, and then select the rollback check box. To do so, perform the following steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, and then click **Patches and Updates**.

2. On the Patches and Updates page, in the Patch Search region, enter the **patch number** that you want to rollback.
3. In the **Add Patch to Plan** dialog box, enter a unique name for the plan, and select all the targets from where you want to rollback the patches.
4. Click **Create Plan**.
5. In the Create Plan Wizard, select **Deployment Options**.
6. On the Deployment options page, in the Rollback section, select **Specify if you want to rollback the patches in this plan**, and click **Next**.
7. On the Validation page, click **Analyze** to validate the plan. After a successful analysis, click **Next**.
8. On the Review and Deploy page, review the details you have provided for the patch plan, and then click **Deploy** to rollback the selected patch from the corresponding targets mentioned in the plan.

Patching Linux Hosts

This chapter explains how you can patch Linux hosts using Oracle Enterprise Manager Cloud Control (Cloud Control). In particular, this chapter covers the following:

- [Overview of Patching Linux Hosts](#)
- [Understanding the Deployment Procedure for Patching Linux Hosts](#)
- [Supported Linux Releases](#)
- [Setting Up Infrastructure for Linux Patching](#)
- [Patching Linux Hosts](#)
- [About Linux Patching Home Page](#)
- [About Configuration File Management](#)

Note: To understand how you can use Enterprise Manager Ops Center to update or patch the Linux hosts, refer to the chapter on updating operating systems in the *Oracle Enterprise Manager Ops Center Provision and Update Guide*.

25.1 Overview of Patching Linux Hosts

Linux Host Patching is a feature in Cloud Control that helps in keeping the hosts in an enterprise updated with security fixes and critical bug fixes, especially in a data centre or a server farm. This feature support in Cloud Control enables you to:

- Set up Linux RPM Repository based in Unbreakable Linux Network (ULN) channels
- Download Advisories (Erratas) from ULN
- Set up Linux Patching Group to update a group of Linux hosts and collect compliance information
- Allow non-compliant packages to be patched
- Rollback/Uninstall packages from host
- Manage RPM repositories and channels (clone channels, copy packages from one channel into another, delete channels)
- Add RPMs to custom channels
- Manage Configuration file channels (create/delete channels, upload files, copy files from one channel into another)

The following are concepts related to Linux patching:

Linux Host	A host target in Cloud Control that is running the Linux operating system.
Linux Patching Group	A set of managed Linux hosts that are associated with a common RPM repository. Every group is configured with an update schedule according to which, a recurring job is triggered that will update the hosts of the group with the associated RPM repositories.
Unbreakable Linux Network (ULN)	Unbreakable Linux Network (ULN) is a Web site hosted by Oracle to provide updates for Oracle Linux.
ULN Channel	A channel is a grouping of RPM packages on the ULN network. For example, <code>el4_latest</code> channel contains all packages for OEL 4.
RPM Repository	RPM repository is a directory that contains RPM packages and their metadata (extracted by running <code>yum-arch</code> and <code>createrepo</code>). The RPM repository is accessible via <code>http</code> or <code>ftp</code> . An RPM repository can be organized to contain packages from multiple channels. For example, <code>/var/www/html/yum/Enterprise/EL4/latest</code> might contain packages from the <code>el4_latest</code> channel on ULN.
Custom Channel	A channel that is created by the user to store a set of custom RPM packages. Custom channels can be added to the RPM repository.
Configuration Channel	A channel that is created by the user to store a set of Linux configuration files. Configuration channels can be used in the Linux patching application GUI to deploy configuration files on Linux hosts.

25.2 Understanding the Deployment Procedure for Patching Linux Hosts

Cloud Control provides the following deployment procedures for Linux patching:

- *Patch Linux Hosts*
This deployment procedure enables you to patch Linux hosts.
- *Linux RPM Repository server setup*
This deployment procedure enables you to set up a Linux RPM repository server. To set up the Linux RPM repository server, refer to [Section 25.4.2.2](#).

25.3 Supported Linux Releases

The following releases are supported for Linux patching:

Table 25–1 Supported Releases

Feature	Linux Distributions Supported
Compliance	Oracle Linux 4, Oracle Linux 5, Oracle Linux 6 Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6

Table 25–1 (Cont.) Supported Releases

Feature	Linux Distributions Supported
Update Job	Oracle Linux 4, Oracle Linux 5, Oracle Linux 6 Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6 SuSE Linux
Emergency Patching	Oracle Linux 4, Oracle Linux 5, Oracle Linux 6 Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6
Linux Patching Deployment Procedures	Oracle Linux 4, Oracle Linux 5, Oracle Linux 6 Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6 SuSE Linux
Undo Patching	Oracle Linux 4, Oracle Linux 5, Oracle Linux 6 Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6
Channel management	Oracle Linux 4, Oracle Linux 5, Oracle Linux 6 Red Hat Enterprise Linux 4, Red Hat Enterprise Linux 5, Red Hat Enterprise Linux 6

25.4 Setting Up Infrastructure for Linux Patching

This section describes the setup requirements for Linux patching. In particular, this section describes the following:

- [Meeting Prerequisites for Using the Linux Patching Feature](#)
- [Setting Up the RPM Repository](#)
- [Setting Up Linux Patching Group for Compliance Reporting](#)

25.4.1 Meeting Prerequisites for Using the Linux Patching Feature

To use the Linux Patching feature, meet the following prerequisites:

1. Meet the basic prerequisites described in [Chapter 2](#).
2. Deploy the PAR files from the Oracle Management Service (OMS) host:


```
${OMS_ORACLE_HOME}/bin/PARDeploy -action deploy -parDir
```
3. Install yum or up2date on all target hosts, and enable SUDO for the patch user.
4. Ensure that the patch user credentials to be used for patching have *write* access under Oracle home directory of the Management Agent.
5. Ensure that the operating system credentials used to create groups and set up repository have SUDO as root privilege.
6. Enable the following commands through SUDO:
 - /bin/cp
 - /bin/rm
 - /bin/chmod
 - /sbin/chkconfig

- yum
- up2date
- sed
- rpm

25.4.2 Setting Up the RPM Repository

This section describes how you can set up the RPM repository. In particular, this section describes the following:

- [Prerequisites for Setting Up the RPM Repository](#)
- [Setting Up the RPM Repository](#)

25.4.2.1 Prerequisites for Setting Up the RPM Repository

Before setting up the RPM repository, meet the following prerequisites:

1. Identify a Redhat or OEL host, install a Management Agent, and point to the OMS. This host must have the *sudo* package installed.
2. Obtain a valid Customer Support Identifier (CSI) number from your Oracle sales representative.
3. Download the up2date packages corresponding to the host version and release from <https://linux.oracle.com/switch.html>.
4. Upload the up2date packages to the Software Library.

Note: For a multi-OMS setup, the following steps only need to be performed on one OMS.

- First compress up2date and up2date-gnome into a zip file and name it as up2date_comp.zip.
- Copy the zip file to the <ORACLE_HOME>/sysman/metadata/swlib/patch/stageServerComponents directory present in the Oracle home of the OMS.
- Edit the Patch Software Library entities metadata file swlib.xml under the <ORACLE_HOME>/sysman/metadata/swlib/patch directory present in the Oracle home of the OMS to upgrade the ExternalID of the Software Library entity **Up2date Package Component**.
- Upload the zip file to Software Library by running the following command:

```
$ emctl register oms metadata -service swlib -file $ORACLE_HOME/sysman/metadata/swlib/patch/swlib.xml -core
```
- 5. Ensure that ULN staging host is able to communicate with the ULN network. If proxy is required, up2date from the host needs to be configured as well. The connectivity with ULN will be detrimental for up2date -register -nox command.
- 6. Patch user (OS credentials used to setup the staging server) must have write permission under the agent home. Patch user must also have SUDO privilege.

25.4.2.2 Setting Up the RPM Repository

To set up an RPM Repository that downloads latest RPM packages and advisories from ULN, follow these steps.

1. In Cloud Control, from the **Setup** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Patching Setup page, in the **Linux Patching Setup** tab, click **Setup RPM Repository**.
3. On the Setup RPM Repository page, in the RPM Repository Server section, select the RPM Repository server by clicking the search icon. Select the host assigned for subscribing to ULN.
4. In the Credentials section, enter the user name and password to use. Click **Apply**.
5. In the Deployment Procedure submission confirmation, click **Linux RPM Repository Server Setup**. The deployment procedure starts a job to download latest RPM packages and Advisories from the subscribed ULN channels.
6. (Optional) If you want to change the refresh mode to 30 seconds, then from the **View Data** list, select **Real Time: 30 Second Refresh**.
7. In the Steps tab of the Status Detail section, check the status of this step. Wait till the step **Installing Up2date** is completed or skipped.
8. Click the status of the step **Register with ULN**. In the Phase Status page, do the following:
 - a. Log in to the RPM Repository server machine.
 - b. Configure up2date to use a proxy server, if any, by following the instructions at:
https://linux.oracle.com/uln_faq.html - 9
 - c. Register the host to ULN by following the steps at:
https://linux.oracle.com/uln_faq.html - 2

Note: While registering, you can choose the user name and password. This credential will be used to log in to <http://linux.oracle.com>

- d. After registering the host, select the target and click **Confirm**, and then click **Done** to go to the main flow.
9. Click the status of the step **Subscribe to ULN channels**. In the Phase Status page, do the following:
 - a. When you register a server, it will be subscribed to a channel that has the latest Enterprise Linux packages for the appropriate architecture. To subscribe to additional channels, log in to <http://linux.oracle.com> after you register your system. Click on the **Systems** tab to manage subscriptions for each subscribed server.
 - b. Subscribe either to el*_addon channel (this channel contains createrepo) or manually install the createrepo package.
 - c. Type the command `up2date -nox -show-channels` to verify the list of subscribed channels.

10. Once the deployment procedure ends successfully, from the **Setup** menu, select **Provisioning and Patching**, then select **Linux Patching**.
11. On the Patching Setup page, in the **Linux Patching Setup** tab, click **Manage RPM Repository** to verify if the ULN channels are displayed in the Cloud Control console.
12. On the Manage RPM Repository page, check if all the subscribed channels are listed and if all the packages are downloaded.

25.4.3 Setting Up Linux Patching Group for Compliance Reporting

This section describes how you can set up a Linux Patching group for compliance reporting by associating the group with the RPM Repository (each subscribed ULN channel is a repository) created in [Section 25.4.2](#).

In particular, this section describes the following:

- [Prerequisites for Setting Up Linux Patching Group](#)
- [Setting Up a Linux Patching Group](#)

25.4.3.1 Prerequisites for Setting Up Linux Patching Group

Before setting up the Linux Patching Group, meet the following prerequisites:

- RPM Repository server must be set up or a custom RPM Repository must be set as a channel in Cloud Control.
- Yum or up2date should be installed in the target hosts.
- Sudo must be installed on the target hosts.
- You must have Operator privileges on the hosts that you want to add to the Linux host patching group.
- Patch user must have write access under the agent home. Patch user must have sudo privilege.

25.4.3.2 Setting Up a Linux Patching Group

To set up a Linux patching group, do the following:

1. In Cloud Control, from the **Setup** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Patching Setup page, in the **Linux Patching Setup** tab, click **Setup Groups**.
3. On the Setup Groups page, click **Create**.
4. On the Create Group: Properties page, enter a unique name for the group. Select the maturity level, Linux distribution, and Linux hosts to be added to the group.
5. Click **Next**.
6. On the Create Group: Package Repositories page, select the RPM Repositories to be associated with the group (click the search icon to select repository).

Select **Automatically Update Hosts** if you want to auto-update the host, that is, to schedule an update job (schedule specified as one of the subsequent step) to update all non-compliant packages from the selected package repository.

Under the Package Compliance section, choose whether to include *Rogue* packages in compliance reporting or not.

7. Click **Next**.

8. On the Create Group: Credentials page, enter the host credentials or choose to use preferred credentials.
9. Click **Next**.
10. On the Create Group: Patching Script page, enter any pre/post patching operations to be done. This is not a mandatory step.

Note: Steps (10), (11), (12), (13) will be skipped if **Automatically Update Hosts** was not selected.

11. Click **Next**.
12. On the Schedule page, set the schedule for the update job.
13. Click **Next**.
14. On the Review page, validate all the parameters.
15. Click **Finish**.

Note: If you had not selected the **Automatically Update Hosts** option, then three jobs are submitted. If the option was selected, then four jobs are submitted. [Table 25–2](#) explains the jobs submitted. Follow the jobs submitted by clicking the job’s link.

16. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Linux Patching**. Verify the compliance report generated. The group created will have at least one out-of-date package.

Table 25–2 *Jobs Submitted for Setting Up Linux Patching Group*

Job	Description
Patching Configuration	This job configures all the hosts for patching. It creates configuration files to be used by yum and up2date tool.
Compliance Collection	Compares the packages already installed in the machine with the packages versions in the selected RPM Repositories and generates Compliance Reports.
Package Information	Collects metadata information from the selected RPM Repositories.
Packages Update	Updates non-compliant packages.

25.5 Patching Linux Hosts

To the patch the Linux hosts, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Deployment Procedure Manager page, in the Procedure Library tab, select **Patch Linux Hosts**, and click **Launch**.
3. On the Package Repository page, in the LINUX Distribution section, select the correct distribution and also select the update tool to use.
4. In the Package Repository section, click the torch icon to select the RPM Repository.

5. Click **Next**.
6. On the Select Updates page, select the packages to be updated.
7. Click **Next**.
8. On the Select Hosts page, select the targets to be updated. You can also select a group by changing the target type to group.
9. Click **Next**.
10. On the Credentials page, enter the credentials to be used for the updates.
11. Click **Next**.
12. On the Pre/Post script page, enter the pre/post scripts, if any.
13. Click **Next**.
14. On the Schedule page, enter the schedule to be used.
15. Click **Next**.
16. On the Review page, review the update parameters. Click **Finish**.
17. A deployment procedure is submitted to update the selected packages. Follow all the steps of the procedure until it completes successfully.

25.6 About Linux Patching Home Page

This section describes the following tasks you can perform on the Linux Patching Home page:

- [Viewing Compliance History](#)
- [Patching Non-Compliant Packages](#)
- [Rolling Back or Deinstalling Packages](#)
- [Registering a Custom Channel](#)
- [Cloning a Channel](#)
- [Copying Packages from One Channel to Another](#)
- [Adding Custom Packages to a Channel](#)
- [Deleting a Channel](#)

25.6.1 Viewing Compliance History

This section describes how you can view the compliance history for a selected group, for a specific time period. In particular, this section covers the following:

- [Prerequisites for Viewing Compliance History](#)
- [Viewing Compliance History](#)

25.6.1.1 Prerequisites for Viewing Compliance History

- Ensure that you have defined at least one Linux patching group.
- Ensure that you have *View* privileges on the Linux host comprising the patching group.

25.6.1.2 Viewing Compliance History

To view the compliance history of a Linux patching group, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Compliance Home page, from the Related Links section, click **Compliance History**.
3. On the Compliance History page, the Groups table lists all the accessible Linux patching groups and the number of hosts corresponding to each group.
4. If there are multiple Linux patching groups, the Compliance History page displays the historical data (for a specific time period) for the first group that is listed in that table.
5. To view the compliance history of a Linux patching group, click the View icon corresponding to that group.

Note: By default, the compliance data that is displayed is retrieved from the last seven days. To view compliance history of a longer time period, select an appropriate value from the View Data drop-down list. The page refreshes to show compliance data for the selected time period.

25.6.2 Patching Non-Compliant Packages

This section describes how you can patch non-compliant packages from the Linux Patching home page. In particular, this section covers the following:

- [Prerequisites for Patching Non-Compliant Packages](#)
- [Patching Non-Compliant Packages](#)

25.6.2.1 Prerequisites for Patching Non-Compliant Packages

Before patching non-compliant packages, ensure that a Linux Patching group is created and the Compliance Collection job has succeeded.

25.6.2.2 Patching Non-Compliant Packages

To patch non-compliant packages, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Linux Patching page, in the Compliance Report section, select the Group and click **Schedule Patching**.
3. In the Patch Linux Hosts Wizard, provide the required details in the interview screens, and click **Finish** on the Review page.
4. A deployment procedure is submitted to update the host. Check if all the steps finished successfully.

25.6.3 Rolling Back or Deinstalling Packages

Note: Rolling back upgrades is supported to a certain extent. When performing an upgrade such as from OEL 5.2 to OEL 5.3, many RPMs that are dependent on others are upgraded. When you apply RPMs, this dependency can be followed. However, when rolling back patches, this dependency must be followed in reverse order. This reverse operation is not supported by YUM or up2date. Hence, you can use the rollback feature to rollback one or two packages, but not to completely rollback a major upgrade such as from OEL 5.2 to OEL 5.3.

This section describes how you can rollback a patch to its previous stable version, or even uninstall the unstable version completely in case that patch version is found unsuitable for has a bug or security vulnerability. In particular, this section covers the following:

- [Prerequisites for Deinstalling Packages](#)
- [Rolling Back or Deinstalling Packages](#)

25.6.3.1 Prerequisites for Deinstalling Packages

Before rolling back or deinstalling the packages, meet the following prerequisites:

- Ensure that a Linux Patching group is created.
- Ensure that the lower version of the package is present in the RPM repository.

25.6.3.2 Rolling Back or Deinstalling Packages

To roll back or uninstall the packages, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Linux Patching page, in the Compliance Report section, select a group, and click **Undo Patching**.
3. On the Undo Patching: Action page, select an appropriate option:
 - **Uninstall Packages**, deinstalls a package.
 - **Rollback Packages**, rolls back to an earlier version/release of a package. To perform this operation, more than one version/release of that package should be present in the packages repositories.
 - **Rollback Last Update Session**, reverts the effects of the previous patch update session.
4. Click **Next**.
5. Provide the required details in the wizard, and on the Review page, click **Finish**.
6. A job is submitted to rollback the updates done in the previous session.
7. Examine the job submitted to see if all the steps are successful.

25.6.4 Registering a Custom Channel

This section describes how you can register a custom channel. In particular, this section covers the following:

- [Prerequisites for Registering a Custom Channel](#)
- [Registering a Custom Channel](#)

25.6.4.1 Prerequisites for Registering a Custom Channel

Before registering a custom channel, meet the following prerequisites:

- Ensure that the RPM Repository is under `/var/www/html` and is accessible through HTTP protocol.
- Ensure that metadata files are created by running `yum-arch` and `createrepo` commands.
- Ensure that a Management Agent is installed on the RPM repository host, and ensure that Management Agent is communicating with the OMS.

25.6.4.2 Registering a Custom Channel

To register a custom RPM Repository, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Patching Setup page, in the Linux Patching Setup tab, click **Manage RPM Repository**.
3. On the Manage Repository Home page, click **Register Custom Channel**.
4. On the Register Custom Channel page, enter a unique channel name.
5. Click **Browse** and select the host where the custom RPM repository was setup.
6. Enter the path where RPM repository resides. The directory location must start with `/var/www/html/`.
7. Click **OK**.

A Package Information job is submitted. Follow the job until it completes successfully.

25.6.5 Cloning a Channel

This section describes how you can clone a channel. In particular, this section covers the following:

- [Prerequisites for Cloning a Channel](#)
- [Cloning a Channel](#)

25.6.5.1 Prerequisites for Cloning a Channel

Before cloning a channel, meet the following prerequisites:

1. Ensure that there is at least one channel already present.
2. Ensure that the patching user has *read/write* access on both the source and target channel hosts.
3. Ensure that there is enough space on the target channel host.
4. Ensure that the patch user has *write* access on the agent home. Also ensure that the patch user has SUDO privileges.

25.6.5.2 Cloning a Channel

To clone a channel, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Patching Setup page, in the Linux Patching Setup tab, click **Manage RPM Repository**.
3. On the Manage RPM Repository page, select the source channel you want to clone, and click **Create Like**.
4. Enter the credentials to use for the source channel. The credentials must have both read and write access.
5. Enter a unique target channel name.
6. Click **Browse** to select the target host name.
7. Enter the directory location of the target channel. This directory should be under `/var/www/html`.
8. Enter the credentials to use for the target channel. This credential should have both read and write access.
9. Click **OK**.

A Create-Like job is submitted. Follow the job until it completes successfully.

25.6.6 Copying Packages from One Channel to Another

This section describes how you can copy packages from one channel to another. In particular, this section covers the following:

- [Prerequisites for Copying Packages from One Channel to Another](#)
- [Copying Packages from One Channel to Another](#)

25.6.6.1 Prerequisites for Copying Packages from One Channel to Another

Before copying the packages from one channel to another, meet the following prerequisites:

1. Ensure that there are at least 2 channels.
2. Ensure that the patching user has *read/write* access on both the source and target channel hosts.
3. Ensure that the target channel machine has adequate space.
4. Ensure that the patch user has *write* access on the agent home. Also ensure that patch user has SUDO privilege.

25.6.6.2 Copying Packages from One Channel to Another

To copy the packages from one channel to another, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Patching Setup page, in the Linux Patching Setup tab, click **Manage RPM Repository**.
3. On the Manage RPM Repository page, select the source channel, and click **Copy Packages**.

4. Select the target channel.
5. From the source channel section, select and copy the packages to the target channel section.
6. Enter credentials for the source and target channels. These credentials should have read/write access to the machines.
7. Click **OK**.

A Copy Packages job is submitted. Follow the job until it completes successfully.

25.6.7 Adding Custom Packages to a Channel

This section describes how you can add custom packages to a channel. In particular, this section covers the following:

- [Prerequisites for Adding Custom Packages to a Channel](#)
- [Adding Custom Packages to a Channel](#)

25.6.7.1 Prerequisites for Adding Custom Packages to a Channel

Before you add custom packages to a channel, meet the following prerequisites:

1. Ensure that there is at least one channel.
2. Ensure that the patching user has *write* access on the channel host.
3. Ensure that the patch user has *write* access on the agent home. Also ensure that the patch user has SUDO privilege.

25.6.7.2 Adding Custom Packages to a Channel

To add custom RPMs to a channel, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Patching Setup page, in the Linux Patching Setup tab, click **Manage RPM Repository**.
3. On the Manage RPM Repository page, select the channel name where you want to add the RPM, and click **Add**.
4. Select the source target name and the credentials to be used for the host. The credentials you use must have read/write access.
5. On the Upload Files section, click the search icon to browse for the RPM files.
6. Enter the credentials to be used on the channel's host.
7. Click **OK**.

An Add Package job is submitted. Follow the job until it completes successfully.

25.6.8 Deleting a Channel

This section describes how you can delete a channel. In particular, this section covers the following:

- [Prerequisites for Deleting a Channel](#)
- [Deleting a Channel](#)

25.6.8.1 Prerequisites for Deleting a Channel

Before deleting a channel, meet the following prerequisites:

1. Ensure that there is at least one channel.
2. Ensure that the patching user has *write* access to delete the RPM files from the channel host.
3. Ensure that the patch user has *write* access on the agent home. Also, ensure that the patch user has SUDO privileges.

25.6.8.2 Deleting a Channel

To delete a channel, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Patching Setup page, in the Linux Patching Setup tab, click **Manage RPM Repository**.
3. On the Manage RPM Repository page, select the channel name you want to delete, and click **Delete**.
4. If you want to delete the packages from the RPM Repository machine, select the check box and enter the credentials for the RPM Repository machine. Click **Yes**.
5. If you have not selected to delete the packages from RPM Repository machine, you will get a confirmation message stating *Package Channel <channel name> successfully deleted*. If you have selected the **Delete Packages** option, a job will be submitted to delete the packages from the RPM Repository machine. Follow the job until it completes successfully.

25.7 About Configuration File Management

This section describes how you can perform the following configuration file management activities:

- [Prerequisites for Managing Configuration File](#)
- [Creating Configuration File Channel](#)
- [Uploading Configuration Files](#)
- [Importing Configuration Files](#)
- [Deploying Configuration Files](#)
- [Deleting Configuration File Channels](#)

25.7.1 Prerequisites for Managing Configuration File

Ensure that the Software Library is already configured on the OMS.

25.7.2 Creating Configuration File Channel

To create a configuration file channel, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Linux Patching page, click the **Configuration Files** tab.
3. In the Configuration Files tab, click **Create Config File Channel**.

4. On the Create Configuration File Channel page, enter a unique channel name and description for the channel, and click **OK**.

You will see a confirmation message saying that a new configuration file is created.

25.7.3 Uploading Configuration Files

This section describes how you can upload configuration files. In particular, this section covers the following:

- [Prerequisites for Uploading Configuration Files](#)
- [Uploading Configuration Files](#)

25.7.3.1 Prerequisites for Uploading Configuration Files

Before uploading configuration files, ensure that there is at least one configuration file.

25.7.3.2 Uploading Configuration Files

To upload configuration files, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Linux Patching page, click the **Configuration Files** tab.
3. In the Configuration Files tab, select the configure file you want to upload, and click **Upload Configuration Files**.
4. Select an appropriate upload mode. You can either upload files from local host (where the browser is running) or from a remote host (agent should be installed on that host and that agent should be communicating with this OMS).
5. In the File Upload section, enter the file name, path where the file will be deployed in the target host, and browse for the file on the upload host.
6. For uploading from remote machine, click **Upload from Agent Machine**. Click **Select Target** and select the remote machine.

Before browsing for the files on this machine, set preferred credential for this machine.

7. After selecting the files, click **OK**.

You will see a confirmation message that states that files have been uploaded.

25.7.4 Importing Configuration Files

This section describes how you can import configuration files. In particular, this section covers the following:

- [Prerequisites for Importing Configuration Files](#)
- [Importing Configuration Files](#)

25.7.4.1 Prerequisites for Importing Configuration Files

Before importing configuration files, ensure that there are at least two channels.

25.7.4.2 Importing Configuration Files

To import configuration files, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Linux Patching page, click the **Configuration Files** tab.
3. In the Configuration Files tab, select the source channel, and click **Import Files**.
4. Select the target channel.
5. From Source channel section, select the files and copy it to the target channel section. Click **OK**.

You will see a confirmation message stating that the selected files have been imported successfully.

25.7.5 Deploying Configuration Files

This section describes how you can deploy configuration files. In particular, this section covers the following:

- [Prerequisites for Deploying Configuration Files](#)
- [Deploying Configuration Files](#)

25.7.5.1 Prerequisites for Deploying Configuration Files

Before deploying configuration files, meet the following prerequisites:

- Ensure that the patch user has *write* access on the agent home. Also ensure that the patch user has SUDO privilege.
- Ensure that there is at least one channel with some files uploaded.

25.7.5.2 Deploying Configuration Files

To deploy files, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Linux Patching page, click the **Configuration Files** tab.
3. In the Configuration Files tab, select the source channel, and click **Deploy Files**.
4. In the wizard that appears, select the files you want to deploy, and click **Next**.
5. Click **Add** to select the targets where you want to deploy the files.
6. Enter the credentials for the selected targets.
7. Enter the Pre/Post scripts you want to run before or after deploying the files.
8. Review the deploy parameters and click **Finish**.

A deploy job is submitted. Follow the job's link until it completes successfully.

25.7.6 Deleting Configuration File Channels

This section describes how you can delete configuration file channels. In particular, this section covers the following:

- [Prerequisites for Deleting Configuration File Channels](#)
- [Deleting Configuration File Channels](#)

25.7.6.1 Prerequisites for Deleting Configuration File Channels

Before deleting a configuration file channel, ensure that there is at least one configuration file.

25.7.6.2 Deleting Configuration File Channels

To delete a configuration file channel, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Linux Patching**.
2. On the Linux Patching page, click the **Configuration Files** tab.
3. In the Configuration Files tab, select the channel, and click **Delete**. Click **Yes**.

You will see a configuration message stating that the channel was successfully deleted.

Part VIII

Configuration, Compliance, and Change Management

This part contains the following chapters:

- [Chapter 26, "Managing Configuration Information"](#)
- [Chapter 27, "Managing Compliance"](#)
- [Chapter 28, "Managing Database Configuration Changes"](#)
- [Chapter 29, "Additional Setup for Real-time Monitoring"](#)

Managing Configuration Information

This chapter explains how Oracle Enterprise Manager Cloud Control (Cloud Control) simplifies the monitoring and management of the deployments in your enterprise.

This chapter covers the following:

- [Overview of Configuration Management](#)
- [Overview of Configuration Searches](#)
- [Overview of Configuration Browser](#)
- [Overview of Configuration History](#)
- [Overview of Comparisons and Templates](#)
- [Overview of Custom Configurations and Collections](#)
- [Overview of Parsers](#)
- [Overview of Client Configurations](#)
- [Overview of Relationships](#)
- [Overview of Configuration Topology Viewer](#)

26.1 Overview of Configuration Management

Cloud Control collects configuration information for all managed targets across the enterprise. Collected configuration information is periodically sent to the Management Repository over HTTP or HTTPS, allowing you to access up-to-date configuration information for your entire enterprise through Cloud Control.

Cloud Control enables you to view, save, track, compare, search, and customize collected configuration information for all managed targets known to Enterprise Manager. Additionally, the Configuration Topology Viewer provides a visual layout of a target's relationships with other targets; for example, you can determine a system's structure by viewing the members of a system and their interrelationships.

[Table 26–1](#) provides a snippet of configuration information collected for a small sampling of target types as an example.

Table 26–1 Collected Configurations for Various Targets

Target Type	Collected Configuration Information
Host ¹	<ul style="list-style-type: none"> ■ Hardware (includes memory, CPU, I/O device, and network information) ■ Operating system (includes installed patches and patch sets) ■ Oracle software (includes installed products and their components, patch sets, and interim patches applied using OPatch) ■ Other software (includes all software registered with the operating system)
Database ²	<ul style="list-style-type: none"> ■ Database and instance properties ■ Initialization and System Global Area parameters ■ Tablespace, datafile, and control file information ■ Redo logs, rollback segments, and high availability information ■ Licensing information
Middleware such as WebLogic Server	<ul style="list-style-type: none"> ■ Node Manager, machine, Web service, and Web service port configurations ■ Resource Adapter, including outbound ■ Web and EJB modules ■ Server information ■ JDBC Datasource and Multi Datasource ■ Resource usage ■ Virtual hosts ■ Startup Shutdown classes ■ Jolt Connection Pool ■ Work Manager ■ JMS Topic, Queue and Connection Factory ■ Network channels
Elastic Cloud Infrastructure	<ul style="list-style-type: none"> ■ Switch details ■ Storage appliance details ■ Compute node details (including associated "Host" target GUID) ■ Switch ports configuration ■ Network topology (switch port - device association metric)
VM Server Pool	<ul style="list-style-type: none"> ■ Server Pool configuration details (total disk space and memory available, for example) ■ VM Guest member details <p>VM Server member details</p>
Client ³	<ul style="list-style-type: none"> ■ Hardware ■ Operating system (includes properties, file systems, patches) ■ Software registered with the operating system ■ Network data (includes latency and bandwidth to the Web server) ■ Client-specific data that describes configuration for the browser used to access the client configuration collection applet ■ Other client-oriented data items

Table 26–1 (Cont.) Collected Configurations for Various Targets

Target Type	Collected Configuration Information
Non-Oracle Systems	<ul style="list-style-type: none"> ■ Hardware details including vendor, architecture, CPU, and I/O device information. ■ Operating system details including name, version, software and package lists, kernel parameters, and file system information. ■ OS Registered software including product name, vendor, location, and installation time.

¹ The default collection period for host configuration information is 24 hours.

² The default collection period for database configuration information is 12 hours.

³ Refer to [Section 26.8](#) in this chapter for more information.

Use Cloud Control to manage enterprise configurations:

- Search collected configuration data
- Compare configurations
- View latest and saved configurations as well as inventory and usage details
- Monitor configuration history for changes
- Build custom configurations and introduce custom target types
- Collect and analyze external client configurations
- Perform root cause analysis and impact analysis

26.2 Overview of Configuration Searches

Use configuration search to search configuration data across the enterprise. Cloud Control ships with a set of out-of-box configuration searches, which you can use as a starting point to explore the volume of configuration data collected. As you work with a provided search, you can tailor the search criteria to refine or broaden the results, and save the altered search under a new name.

Perform powerful searches across the enterprise using sophisticated combinations of search filters, options, and relationships. Consider these search examples:

- Show all hosts with dual core CPUs
- Show all tablespaces having at least one 100 MB datafile
- Show all Oracle Homes installed on Linux 5.6 hosts
- Show all targets monitored by a particular Management Agent
- Find all database instances with initialization parameters p1 and p2 having values v1 and v2, respectively

Enhance the search filtering criteria by adding your own SQL query statements. Save interesting search results by printing a report or exporting to a file.

To access the search capability, from the **Enterprise** menu select **Configuration**, then select **Search**. See the Cloud Control online help for information on setting up and executing configuration searches.

This section covers the following topics:

- [Managing Configuration Searches](#)
- [Setting Up a Search](#)

- [Reviewing Search Scenarios](#)

26.2.1 Managing Configuration Searches

The Configuration Search library contains Oracle-supplied and user-created configuration searches that you can use as-is or as the basis for similarly conceived searches. Or, you can elect to create searches from scratch.

To access the Configuration Search library, From the **Enterprise** menu, select **Configuration**, then select **Search**.

Search for any existing configuration searches for all target types, or use the criteria to narrow the search. The search name and owner fields recognize containment, so you can specify a text string as a partial name to find all searches whose name or owner contains the string. When you click Search, the results appear in a table at the bottom of the page.

Select a configuration search in the library and click **Run** to execute the search. A new page appears that reflects the search parameters applied in the search execution, with the results, if any, displayed at the bottom of the page.

Perform these additional tasks:

- To edit an existing configuration search, select a search in the table and click **Edit**. A new page appears displaying the search parameters that constitute the search. Change the search criteria to achieve the desired results. When you are satisfied, save the search. **Save** overwrites the existing search. **Save As** enables you to save the edited search under a new name. If you are working with an Oracle-provided search, use save as.
- To create a new search based on an existing search, select a search in the table and click **Create Like**. Specify a name for the copied search in the dialog that opens. Select the new row in the table and click **Edit**. Make the desired changes to the search parameters and save under the new name.
- To delete an existing search, select a search in the table and click **Delete**. In the dialog that opens, confirm the operation. You must be owner or an administrator to delete a search. A search in use cannot be deleted. Oracle recommends that you not delete an out-of-box search.

26.2.2 Setting Up a Search

Use these instructions to create, create-like, or edit a configuration search.

1. Specify basic criteria; you may have to expand the **Commonly Used Search Criteria** to do so. When you select a target type, your selection drives the list of values for the other criteria; for example, available configuration items for the target type you have chosen.

Select a system or group if you want to search target types that are members. Or search for all target types on a specific host.
2. Click **Add Relationships** to associate the target type with other targets. For example, you may want to know the Management Agent that is monitoring a host you have selected.
3. Use built-in flexibility to add property filtering criteria:
 - You can select a configuration item from the drop-down list. This populates the page with field entries for all properties within the item.

- Click **Add Properties** on the right. This opens a dialog where you can drill down within a given configuration item and select specific properties to include as filtering criteria.

So, for example, for target type host you could select the File Systems configuration item from the drop-down list and get property filters for all six properties. Or, you could click **Add Properties** and drill down in the dialog (File Systems under Operating System) to select specific filtering properties, for example, Resource Name and Mount Location.

4. For each property filter you add, create an expression by choosing an operator and specifying a value. For example, the configuration item hardware has a core CPU count property. You choose the > operator and specify 2 to filter the search on a core CPU count greater than 2. Operators can take wildcards. Specify % with the contains operator to match on anything.

The green check mark next to each property filter specifies to include the property in the search results. Sometimes, you merely want to take a property value into consideration when searching, but don't want to clutter the results with unnecessary columns. Deselect the properties you don't want to see in the results.

5. Click **Options** at any level to specify whether to match on all or any one of the filters specified at that level, and to further refine what you want to see in the search results.
6. As you add criteria, click **Search** to see the results. Continue to revise the search by adding and removing filters until the results are satisfactory.

Notice in the search results table that the column names are a concatenation of the filters you specify and elect to display. So, for example, If you filter on hardware vendor name for target type host, the column name in the search results table reads Host Hardware Vendor Name.

7. Save the search with a meaningful name; that is, a name that reflects the nature of the configuration search.

Still Not Seeing Expected Results?

Sometimes, despite all the filtering criteria, search results still fall short. To refine the search even further, click **Search Using SQL**. In the dialog that opens, you can edit the SQL Query statement to extend search expressions and rerun the search. Note that you use views in this case; you cannot access the underlying tables. Your SQL edits apply only to the current search execution, so if you want to preserve the edited statement, copy and paste it into a text file for future use.

Options

In addition to setting an and/or condition on filtering, use the Options popup to indicate what you want to see in terms of results. Selection expressions are a concatenation formed on the basis of where the Options popup is invoked. The phrasing of each selection expression relates the option level to its parent.

An example will illuminate what this all means. Suppose the following scenario:

- Select target type database instance
- Add relationship hosted by
- Add hardware CPU filters
- Add property frequency (MHz) > 2000
- Add property ecache (MB) >= 8

If you open the Options popup at the hardware level, the selection radio buttons appear as follows:

- Host and hardware properties that meet the search criteria
- Host where at least one hardware meets the search criteria
- Host where no hardware meets the search criteria
- Host where all hardware meet the search criteria
- Host where not all hardware meet the search criteria

Open the Options popup at the CPUs level and the phrasing changes to Hardware and CPUs..., Hardware where at least one CPUs..., and so forth.

The first selection option returns not only matching entities but also actual property values. The rest return only the matching entities. The nuance between at least one and not all is that the former could conceivably be all, whereas, the latter specifically precludes all.

Options settings appear appended in parentheses at the respective level. So, for example, you might see (Condition:No) (Conjunction:OR) after Hardware, if you set the filter to any and the selection to no hardware meets the search criteria. Note that the order of precedence is top down; that is, settings at the top override settings at lower levels.

Given the scenario, selecting All Filters requires that both CPU property conditions be met to satisfy the criteria.

Dealing with Search Results

If the search results are interesting and worth preserving, you can optionally export and print the results as follows:

- Click **Export** and follow instructions in the export dialog to save the results in a CSV file.
- Click **Print** and select where to print the results.

26.2.3 Reviewing Search Scenarios

A few simple searches are provided below as an exercise in using the interface. The examples assume that you have opened the Configuration Search library and clicked the **Create** button. Explore the out-of-box searches for best practices in setting up a search.

Find All Targets Running on a Specific Host

1. Select **All** as the target type.
2. In the common criteria region, click the **On Host** search icon and locate the specific host.
3. Click the **Search** button to execute the search.

Results appear at the bottom of the page.

Find Database Instances Running on Hosts with More Than Two Core CPUs

1. Select **Database Instance** as the target type.
2. Click **Add Relationships** and in the dialog that opens, select **Hosted By**. Click **OK**.
3. Click **Add Properties** at the host criteria level.

4. In the dialog that opens, expand **Hardware**, select **Core CPU Count**, and click **OK**.
5. Constrain Core CPU Count as: > 2. You may have to scroll down to find the property.
6. Click the **Search** button to execute the search.
Results appear at the bottom of the page.

Find Datafiles Greater Than 100 MB Whose Tablespace Status Is ONLINE

1. Select **Database Instance** as the target type.
2. Click **Add Properties**.
3. In the dialog that opens:
 - a. Expand **Tablespaces** and select **Status**.
 - b. Scroll down, expand **Datafiles**, and select **Size** (Cntrl-click to multiselect).
 - c. Click **OK**.
4. Constrain tablespace status as: `is ONLINE`.
5. Constrain datafiles size as: > 104857600.
6. Ensure that the option to match all conditions is set, then click the **Search** button to execute the search.
Results appear at the bottom of the page.

26.3 Overview of Configuration Browser

Use the Configuration Browser to view configuration data in the context of a single managed entity. Configuration data can include:

- Configuration items and properties
- System configuration data as well as all system members and their configuration data
- System and target relationships (immediate, member of, uses, used by, and so forth)
- Custom configuration collection data

The browser window consists of left and right panes. The left pane is a tree hierarchy. The right pane consists of tabs that display information in tables. As you navigate in the tree, your selection dictates the contents in the right pane. Depending on the selection, tabs appear containing data such as properties and values, relationships, a hierarchical structure of a system and its members, and file contents in both a parsed and raw text format.

You can take any of several actions as you view a configuration in the browser. These actions are available from the **Actions** menu above the tabs. The tree hierarchy in the left pane also has context menus available.

This section covers the following topics:

- [Viewing Configuration Data](#)
- [Working with Saved Configurations](#)
- [Working with Inventory and Usage Details](#)

26.3.1 Viewing Configuration Data

The Configuration Browser enables you to view a target's latest or saved configuration data. While viewing configuration data, you can access configuration features such as compare and history.

1. From the **Targets** menu, select **All Targets**.
2. In the table of returned targets, right-click in the row of the desired target.
3. In the popup menu, select **Configuration**, then select **Last Collected** or **Saved**. In the case of saved configurations, select in the table of saved configurations the one you want to browse, then click **View**. The browser opens to display the (latest or saved) configuration data for the selected target.

Note that these same selections (**Last Collected** and **Saved**) are available in the **Configuration** menu on a target's home page that appears in the top-left corner and typically takes the name of the target type, for example, Host or Web Cache.

4. The browser display differs depending on the target type
 - For standard targets, the tree hierarchy on the left shows the target node at the top, beneath which appear configuration item categories and nested configuration items. Select the target node and the tabs on the right show target properties and various relationships (immediate, member of, uses, used by). Immediate relationships indicate direction: source and destination. Thus, for example, a source target type of database has an immediate relationship (hosted by) with a destination target type of host.

As you traverse the tree on the left, the tab on the right becomes the tree selection and displays the properties and values for the selection in table rows. So, for example, if the target type is host and you select Hardware in the tree on the left, the tab on the right becomes Hardware, and the table row displays values for Host Name, Domain, Vendor Name, and so forth. As the table view changes, look to the lower-right corner to see the number of rows the table contains. For multirow tables, use the search filter to drill down to specific properties and values. Add additional search filters as needed.

- When target type is a system, the tree hierarchy on the left shows the following:
 - The root target at the top level
 - A nested node one level down for each configuration item associated with the root target
 - A folder at the same level as the nested node for each member type
 - A node for each member within the member type beneath the member folder

Select the root target and the tabs on the right show target properties, a system topology table, and various relationships (immediate, member of, uses, used by). Select a configuration item in the tree on the left, and the tab on the right displays the item's properties and values. Note that this applies only to configuration items associated with the root target. Select a member target on the left and the tab on the right displays the member target properties. Note, however, that configuration data for the target does not display.

To see the member target's configuration data, you have to click the **View Last Collected** link above the target properties table. The browser display then becomes the same as for a standard target. There is a bread crumb above the tree hierarchy on the left that enables you to return to the system view. If you

subsequently save the member configuration, the link to the configuration data changes to **Saved Configuration**.

- Select a custom configuration file in the tree on the left; separate tabs for a parsed view and a raw text view of the file appear in the tables on the right.
5. (Optional) If you want to save this configuration snapshot, select **Save Latest** in the **Actions** drop-down menu above the tabs. In the dialog that opens, enter a description by which to distinguish the configuration, then click **Submit Job**. Click **OK** to exit the dialog. The save action is also available on the right-click menu while selecting a target tree node. Saving a configuration saves all the configuration and relationship data for the selected target. It also saves the relationship and configuration data for all member targets.
 6. Other options in the **Actions** menu include:
 - **Go to Homepage**—returns to selected target home page.
 - **Export**—opens a dialog where you can browse to a file location and save the configuration as a CSV file.
 - **Topology**—opens the Configuration Topology Viewer showing the viewed target’s relationships.
 - **Compare**—displays the comparison workflow page, where the viewed target’s configuration is preselected as the one against which to compare other configurations.
 - **Search**—displays the configuration search page where the viewed target is the search object.
 - **History**—displays the history page for the viewed target’s configuration.
 - **Refresh**—triggers a collection of the viewed target’s configuration data and subsequent refresh of the browser’s tree hierarchy. Applicable only when viewing a latest configuration (last collected). Note that a manual refresh on a composite target applies only to the target itself, not to its members.

26.3.2 Working with Saved Configurations

Saved configurations are snapshots in time of collected data preserved for future reference. You may simply want to view the saved data, or you may want to use it as the basis of a comparison.

You can save standard as well as composite configurations. Saving a configuration saves all configuration item and relationship data for the selected target and for all member targets.

Note that there are various ways to save a configuration:

- While viewing a table of all targets, right-click a target and select **Configuration**, then select **Save**.
- While viewing a target’s last collected configuration in the Configuration Browser, select **Save Latest** from the **Actions** drop-down menu.

A save, particularly one that involves systems or groups, can take several minutes. So, for performance reasons, a save action submits a job that occurs asynchronously. To check job status, do the following:

1. From the **Enterprise** menu, select **Job**, then select **Activity**.
2. Click **Advanced Search** and set the following criteria:

- Set **Job Type** to ECM Save (or Save Latest).
 - Set **Target Type** to Targetless.
3. Click **Go**.
 4. Drill down in the search results for save details.

To view a saved configuration:

1. From the **Enterprise** menu, select **Configuration**, then select **Saved**.
2. In the table of saved configurations, select the configuration you want to browse, then click **View**.
3. Navigate the tree hierarchy to expose the following categories of data:
 - Managed entities, configuration items, their properties, and relationships
 - System structures
 - Custom configuration collections

You can also view a saved configuration in the Configuration Browser: right-click a target tree node and select **Configuration**, then select **Saved**.

To compare a saved configuration:

1. From the **Enterprise** menu, select **Configuration**, then select **Saved**.
2. In the table of saved configurations, select the configuration you want to compare against, then click **Compare**.
3. The selected configuration becomes the first configuration in the comparison workflow. Continue the process of setting up the comparison.

To import a previously exported configuration:

1. From the **Enterprise** menu, select **Configuration**, then select **Saved**.
2. Click the **Import** button.
3. In the dialog that opens, browse to the location of the exported configuration data and click **Import**.

Upon refreshing, the imported configuration appears in the table of saved configurations.

26.3.3 Working with Inventory and Usage Details

In the Inventory and Usage Details page you can:

- View inventory summaries for deployments such as hosts, database installations, and fusion middleware installations on an enterprise basis or for specific targets.
- View inventory summary information in the context of different dimensions. For example, for host inventory summary, you can view by platform, vendor, or OS version.
- Drill down multiple levels of inventory details.
- See trends in inventory counts charted across a time line. Chart bars are color-coded to match the view selection.
- Switch to a pie chart to break down the inventory data for the rollup option by color-coded percentages.

- For Hosts (OS Patches) and Databases (Patches Applied), click a patch indicator to link to patch details.
- Repeatedly revise selections to refresh chart and details based on new selections.
- Export deployment and details tables to CSV files.

To view inventory and usage details:

1. From the **Enterprise** menu, select **Configuration**, then select **Inventory and Usage Details**.

Alternatively, you can click **See Details** in the Inventory and Usage region of the Grid Summary page.

2. Select the entity you want to examine and choose a rollup option. For example, show all deployed hosts rolled up by platform. Note that the page refreshes automatically upon selection.
3. For patch updates, click **Yes** to view patch details.
4. Select the radio button to specify how to display the inventory chart.
 - The trend chart shows inventory counts across a time line. Use the magnifier icon to zoom the view. You can adjust the date range by sliding the horizontal scroll bar under the chart.
 - The pie chart breaks down the inventory data for the selected rollup option by percentages in an appealing color-coded visual.
5. Click **Table View** to convert the trend chart to table format. Close the table to return to the chart view.
6. Select one or more rows in the deployments table and click the **View Details** button to refresh the chart and details table based on the selected rows.
7. In any given row in the top table there is a count bar next to the count that represents a percentage of the maximum count. For example, if the maximum number of hosts by platform is four, the bar for hosts represented on two platforms would be half as long. Click the bar to refresh the details table and chart for the row.

Note that you can export either the master (deployments) table or the details table. In either case, click the **Export** button to open a dialog where you can browse to a file location and save the table as a CSV file.

26.4 Overview of Configuration History

Configuration history is a log of changes to a managed entity (target) recorded over a period of one year. The recorded history includes changes both to configurations and to relationships. Relationships are the associations that exist among managed entities.

Configuration history is a powerful tool for monitoring change activity across the enterprise. Consider these use cases:

- You have noticed that an Oracle RAC system has been underperforming for the past month. As an administrator it would be useful to know what changes have occurred during that time. Have members been added or removed? Have there been configuration changes to the system itself?
- The daytime administrator notices that detected changes are the result of a patch having been applied and adds an annotation to that effect. The overnight administrator is alerted to the changes and sees the annotation upon follow-up.

- A hardware memory change to production hosts has been detected. The administrator wants to keep the IT group posted on any future changes in this area. The administrator schedules a recurring job to check history specifically for changes to hardware memory on production hosts and to notify the IT group of such changes.

While viewing a configuration history, you can:

- Track changes to targets over time by specifying and refining search criteria.
- View change history and manipulate how the information is presented.
- Annotate change records with comments that become part of the change history. Annotations have a timestamp and an owner.
- Schedule a history search to capture future changes based on the same criteria.
- View the status of scheduled history jobs.
- Notify others of future change detection.
- Save change history details to a file.

This section covers the following topics:

- [Accessing Configuration History](#)
- [Working with Configuration History](#)
- [Viewing History Job Activity](#)

26.4.1 Accessing Configuration History

Use any of the following methods to access configuration history:

- From the **Enterprise** menu, select **Configuration**, then select **History**. Proceed with a configuration history search.
- Perform a search of all targets. Right-click in a row of returned targets and select **Configuration**, then select **History** in the popup menu. View the results for the selected target, identified by type and name in the respective search criteria fields; change the filtering criteria to see a different result. Select a specific configuration item, for example, or change the date range.
- On a target home page, select **Configuration**, then select **History** in the target type-specific menu (top left corner). View the results for the target, identified by type and name in the respective search criteria fields; change the filtering criteria to see a different result. Select a specific configuration item, for example, or change the date range.

26.4.2 Working with Configuration History

Perform the following tasks within configuration history:

- Drill down within configuration change history
- Enter annotations and comments
- Schedule a recurring history search and send the results
- Save a change history to a file

26.4.2.1 Searching History

Uses various filters to tailor your search of configuration change history.

1. Specify basic search criteria, starting with target type:
 - The **Include Member Target Changes** check box is active only if you select a composite target type (system or group).
 - Click a lookup icon to open a dialog of choices for the respective field. Configuration Item is inactive until you select a target type.
 - The Configuration Item selector contains separate tabs for configuration items and relationships. They are mutually exclusive.
 - Select a time offset from the current date or specify a date range. Default is the last 7 days.
 - Limit the scope of the search to a specific type of change; find only configurations with deleted items, for example.
 - Choose whether to view all criteria-based history records or group them by timestamp and target. The latter is the default.
2. Specify advanced search criteria by selecting from the **Add Filters** drop-down list.
 - The top three selections (**Member of, On Host, Annotation**) are constant. Enter partial text of an annotation, for example, to limit the search to changes commented with the specified text.
 - The rest of the drop-down list depends on the configuration item selected for the target type. Selecting Hardware Network Interface Cards for Host populates the rest of the list with properties appropriate to a NIC.
 - Icons denote key fields in the list. NIC Name is a key field, for example. In general, key fields should remain unchanged over time; that is, the search constraint does not take the form old value new value as nonkey fields do.

Each item you select from the Add Filters list adds a row to the search criteria.
3. Click **Search** to trigger the operation. A progress indicator verifies ongoing search activity. Results appear in the table at the bottom.

Note: One search strategy to consider is perform a gross-level search to see the volume of changes, then go back and refine the search by adding filters.

Working with History Search Results

Each row represents a target satisfying the search criteria in which a change was detected, where a change constitutes something that was added, deleted, or modified. Numbers in parentheses on the tabs reflect the number of respective configuration and relationship changes detected. A search on target name for relationships returns matches on all source targets, destination targets, and targets that contain the target name.

In the changed targets table, select a table row and do any of the following:

- Click **See Real-Time Observations** to search actions monitored by compliance rules. Observations are the actions that users have taken on a host or target that were configured to be monitored through real-time monitoring rules.
- Click **Export** to save the search results to a CSV file such as a spreadsheet. The value in each column represents a comma-separated value.
- Click the number in the History Records column to display the changes detected for the selected target.

In the change details table, select a table row and do any of the following:

- Click **Details** to see the change details in a pop-up window, including old and new values, and the specifics of any annotations. The **Change** link in the Type of Change column pops up the same window.
- Click **See Real-Time Observations** to search actions monitored by compliance rules. Observations are the actions that users have taken on a host or target that were configured to be monitored through real-time monitoring rules.
- Click **Add Annotation** to enter a comment about the change.
- Click **Export** to save the search results to a CSV file such as a spreadsheet. The value in each column represents a comma-separated value.

26.4.2.2 Annotating Configuration Changes

To annotate configuration changes:

1. Select the change row in the results table. To add the same annotation to multiple lines, use the multiselect feature (Ctrl+click or Shift+click).
2. Click the **Add Annotation** button.
3. In the window that pops up, type your comment and click **OK**. Your comment appears in the designated column. Your login name and a timestamp are associated with your comment and available in the pop-up window that opens when you view the change details.

Note that you can also remove an annotation, provided you are the one who entered the comment (or have super administrator privileges). Select the row that contains the annotation and click the **Remove Annotation** button. Confirm the removal in the popup message that opens.

26.4.2.3 Scheduling a History Search and Creating a Notification List

You can schedule the change history search to run as a background job (click the **Schedule and Notify** button). The search can be run once-only or on a recurring basis. Run the search immediately or at some later date. You also can supply e-mail addresses to which to send a link to the search results.

Use a scheduled history search as a tracking mechanism to generate alerts when changes occur.

1. Specify the job schedule:
 - If not now, when. Click **Later** to activate the calendar widget where you can select a date and time.
 - How often. Select report frequency in the drop-down list. Default is once-only.
 - Wait how long. If the job fails to run as scheduled, cancel within a specified time frame.
 - Keep going. Maintain the job schedule for the specified period.
2. Enter the e-mail addresses of those to be directed to the change history search results. Use a comma to separate addresses.
3. Click **OK** to schedule the job.

26.4.2.4 Saving History to a File

You can capture the snapshot of change history you have culled for further review and to share with a wider audience, by saving the change details to a CSV file. Click **Export** and follow instructions in the export dialog.

26.4.3 Viewing History Job Activity

View a list of all current and past history searches. Use search criteria to filter the list of history jobs (click the **History Job Activity** button). For example, show all scheduled history searches started over the past 24 hours; or, show all successful history searches involving hosts started over the past 31 days. The jobs engine purges history jobs older than 31 days

The history jobs you can view beyond your own depend on your role and access level granted.

Select a table row and click **View Result** to go to the Jobs page that reports the history search. From there you can drill down to the changes the history search detected. The job name is a hyperlink that takes you to the same place. Use the bread crumb on the Jobs page to navigate back to the list.

If you are the job owner or otherwise have the proper access level, you can perform list maintenance by deleting history jobs that no longer have relevance.

26.5 Overview of Comparisons and Templates

This section describes the template creation process and the use of rules in the process. It also provides information on setting up comparisons and managing comparison templates.

This section covers the following topics:

- [About Comparison Templates](#)
- [Working with Comparison Templates](#)
- [Specifying Rules](#)
- [About Rules Expression and Syntax](#)
- [Understanding Rules by Example](#)
- [About Comparisons](#)
- [Understanding the Comparison Wizard](#)
- [Working with Comparison Results](#)

26.5.1 About Comparison Templates

A comparison template is an exemplar for fine-tuning a comparison of like configurations. A template is associated with a specific target type, which determines the configuration item types, items, and properties to be compared. A set of default templates ships out of box to support certain target types. A template enables you to establish specific settings to take into account when comparing configurations of the given target type; for example, which property differences to ignore, and which property differences trigger an alert. You also can use constraints to establish acceptable values for specific properties. A configuration being compared that does not comply with the constraint constitutes a difference.

A template can invoke rules, or expressions, to be evaluated in determining when there is a match for comparison purposes, and when to disregard differences detected in a comparison.

Templates can be used as is, or as a guideline. So, for example, you might decide that an existing comparison template, with just a few tweaks, can meet your requirements. Perhaps the template ignores property differences that you are concerned about. In this case, use the create-like feature to make the adjustments to an existing template and save it under another name.

For systems, you design a system template that references member templates, based on the target types that make up the system. Create the member templates before you create the system template.

26.5.2 Working with Comparison Templates

This section describes how to create, edit, and otherwise manage comparison templates.

26.5.2.1 Creating or Editing a Comparison Template

Use these instructions when creating a new template or editing an existing template; this includes create-like.

1. From the **Enterprise** menu, select **Configuration**, then select **Comparison Templates**.

For a new template, click **Create** and provide a name and target type. To base a template on an existing one, select the template row, click **Create Like**, and provide a name. In either case, the action creates a new template row.

2. Select the appropriate template row in the table and click the **Edit** button. The **Template Settings** tab appears.

The compared configurations' target type drives the hierarchy of configuration item types and configuration items on the left. The settings in play for the respective properties on the right derive from the selected template, unless you are creating a new template from scratch, in which case there are no settings.

A system comparison takes an overall template and a template for each system member. Thus there is an additional tab for **Member Settings**. Edit the tab as follows:

- Optionally select the member template to use for each system member type.
 - For any given member type, you can elect not to compare configurations by clearing the check box.
 - For member types that you are comparing, select a target property to use as a matching key. The default is target name, but typically you would want to use a distinguishable property to align comparison entities, such as department or location.
3. In the **Template Settings** tab, select a configuration item type or item in the left pane to expose its properties in the right pane. A key icon denotes a property that is defined as a key column in the configuration item type's metadata.

Tip: Notice the Exclude from Comparison check box column on the **Template Settings** tab. This is a powerful feature that enables you to streamline the comparison by ignoring large chunks of data you don't care about. When you select the check box, the comparison engine disregards the corresponding configuration item type and all of its descendants as if they don't exist when comparing configurations. Contrast this with the ability to ignore individual columns and rows on the **Property Settings** tab (see Step 4), in which the settings are stored as part of comparison results, giving you the option to view the ignored properties on the results page.

So, for example, in comparing host configurations, you may decide that any differences in CPU properties are immaterial. Simply expand the Hardware configuration item type and select the CPUs check box to exclude all properties associated with the item.

4. Click the **Property Settings** tab and check boxes for property differences to be ignored and alerted as appropriate. They are mutually exclusive. When you ignore differences in a property value in this fashion, you are doing so unconditionally for all differences detected in the property value for the configuration item type.

Use a value constraint rule to filter the property value. In this case, the comparison engine compares the property value in the configurations being compared (the second through n configurations) to the constrained value. A property value that fails to satisfy the constraint constitutes a difference. For example, test for a version equal to or greater than 6. Any instance in the compared configurations of a version property value under 6 constitutes a difference. Clearly, you would not set a value constraint if you checked ignore differences. See [Section 26.5.3](#) for details.

5. Repeat the preceding steps to set additional property settings on other configuration items.
6. Optionally, select an item in the left pane and click the **Rules for Matching Instances** tab. For a given property, specify a rule expression to be evaluated to determine when a match exists between configuration instances. In other words, if the expression resolves to true, compare the instances. See [Section 26.5.3](#) for details.

Match rules are column-based; they apply an AND logical operator. If you specify rules for multiple properties, they must all resolve to true to constitute a match.

7. Optionally, select an item in the left pane and click the **Rules for Ignoring Instances** tab. For a given property, specify a rule expression to be evaluated to determine when to ignore differences in configuration instances. In other words, if the expression resolves to true, disregard whatever differences the comparison detects. See [Section 26.5.3](#) for details.

Ignore rules are row-based; they apply an AND logical operator within a subset of rules and an OR logical operator between rule subsets. So, if you specify two rules for property A and two rules for property B, either both rules set on property A OR both rules set on property B must resolve to true to constitute a match.

26.5.2.2 Managing Comparison Templates

In addition to creating and editing comparison templates, you manage them by doing the following:

- View a template's settings and composition; this is read-only

- Delete a template (requires the proper permissions)
- Share templates by exporting them in XML file format and importing them into other Cloud Control systems

View a Comparison Template

You can view out-of-box templates and other users' templates to which you have access. Viewing a template is read-only: you see its makeup, but you cannot change anything, even temporarily.

1. Select a template in the Comparison Templates manager and click the **View** button.
2. Expand items in the tree on the left and peruse the settings and rules on the various tabs.
3. Notice that the **Save** button is disabled. Click **Cancel** to return to the Comparison Templates manager.

Delete a Comparison Template

Deleting a template is subject to the following constraints:

- You cannot delete a comparison template unless you have the proper permissions.
- You cannot delete a default comparison template.
- You cannot delete a comparison template currently in use.

To delete a template, select it in the Comparison Templates manager, click **Delete**, and confirm the operation.

Export a Comparison Template

Use the export feature to save a template as an external file that can be imported into another Cloud Control system.

1. Select a template in the Comparison Templates manager and click the **Export** button.

A platform-specific file dialog opens. For example, if you are using Firefox, the dialog notes that you have chosen to open the named template, which it identifies as an XML file. The dialog asks what you want Firefox to do, open the file in an XML editor or save the file.

2. Select the save radio button and click **OK**.
3. Browse to the desired location in the file system and save the file, changing the name if applicable. You cannot change the name of a default (out-of-box) template on export.

Import a Comparison Template

Any comparison template import must comply with the comparison template .xsd. So, for all intents and purposes, the import should be a previously exported template to ensure compliance.

1. In the Comparison Templates manager click the **Import** button.
2. Browse to the template file location and click **Import**.

The imported template appears as a new row in the template table.

An exported template is associated with its owner. A template whose owner is not the same as the login ID of the person importing the template retains its original

ownership. If you want to be the owner of the imported template, you have to edit the `owner` attribute in the template XML file prior to import, changing the value to your login ID. Or, you can simply remove the attribute, in which case the default owner will be set to the ID of the person initiating the import operation.

The Template Manager disallows import of a default (out-of-box) template of the same name. Similarly, you could change the `name` attribute in the template XML file prior to import to allow the import to occur.

26.5.3 Specifying Rules

Specify rules in the context of creating or editing a comparison template (see [Section 26.5.2.1](#)).

Rules enable you to parse configuration data in order to fine-tune comparisons. In terms of the comparison, a rule applies the expression to the value of the selected item in the configuration instance that is being compared to the benchmark configuration. Matching rules are intended to devise a comparison key that aligns the instances being compared. Ignore rules are intended to establish a basis for disregarding any differences detected between instances being compared.

26.5.3.1 Creating a Value Constraint Rule

Specify value constraint rules as follows:

1. Select a configuration item in the left pane.
2. Click the **Property Settings** tab in the right pane and select the property on which you want to set a value constraint.
3. Click the **Edit Rule** button in the toolbar. In the dialog that opens:
 - a. Select an operator from the drop-down list.
 - b. Type an operands expression, then click **OK**.

To clear a rule, select the table row and click the **Remove Rule** button in the toolbar.

See [Section 26.5.4](#) for details on the formation of a rules expression.

26.5.3.2 Creating a Matching Rule

Specify matching rules as follows:

1. Select a configuration item in the left pane.
2. Click the **Rules for Matching Instances** tab in the right pane, then click **New**.
Click **Show Key Properties** to see which properties are defined as key columns in the selected configuration item type's metadata.
3. Select a property in the drop-down list that appears under **Property Name**.
4. To create the rule, select the table row and click the **Edit Rule** button in the toolbar. In the dialog that opens:
 - a. Select an operator from the drop-down list.
 - b. Type an operands expression, then click **OK**.
 - c. To specify additional rules, click **New** and repeat Steps a and b

To clear a rule, select the table row and click the **Remove Rule** button in the toolbar.

See [Section 26.5.4](#) for details on the formation of a rules expression.

You can enter additional rules for the same or for a different configuration item. When there are multiple rules, they resolve in the order specified. Matching rules take an AND logical operator, which means all conditions must resolve to true to constitute a match.

26.5.3.3 Creating an Ignore Rule

Specify ignore rules as follows:

1. Select a configuration item in the left pane.
2. Click the **Rules for Ignoring Instances** tab in the right pane, then click **New**.
Click **Show Key Properties** to see which properties are defined as key columns in the selected configuration item type's metadata.
3. Select a property in the drop-down list that appears under **Property Name**.
4. To create the rule, select the table row and click the **Edit Rule** button in the toolbar. In the dialog that opens:
 - a. Select an operator from the drop-down list.
 - b. Type an operands expression, then click **OK**.
 - c. To specify additional rules, click **New** and repeat Steps a and b

To clear a rule, select the table row and click the **Remove Rule** button in the toolbar.

See [Section 26.5.4](#) for details on the formation of a rules expression.

You can enter additional rules for the same or for a different configuration item. When there are multiple rules, they resolve in the order specified. Ignore rules take an AND logical operator for rules within a subset, and an OR logical operator between subsets. So, for two subsets, each with multiple rules, all rules in the first subset OR all rules in the second subset must resolve to true to constitute a match.

5. Select **New Or** to indicate the end of one rule subset and the beginning of another.

26.5.4 About Rules Expression and Syntax

A rule consists of an operator and operands. Taken together, they form an expression that resolves to a value that is then compared to the value of the selected item. A true condition satisfies the rule.

Operands can be literals (string literals are enclosed in single quotes), legal numbers, or dates of the form `YYYY-MM-DD HH24:MI:SS.FF`. Operands that directly reference the value of a configuration item must be of the same date type as that value. Operands in square brackets in the syntax are optional.

Operator	Operands
is equal to*	<p>An optional literal value to match; string values are case-sensitive; if unspecified, expression evaluates value of the property to which the rule applies</p> <p>Note that a matching rule compares the values of the configuration items in the respective configuration to one another, not to a third specified value, so the operator does not take an operand in this case.</p> <p>[match-literal]</p>

Operator	Operands
is case-insensitive equal to*	An optional case-insensitive string literal; if unspecified, expression evaluates value of the property to which the rule applies Note that a matching rule compares the values of the configuration items in the respective configuration to one another, not to a third specified value, so the operator does not take an operand in this case. ['match-literal']
is greater than or equal†	A literal value to match; required match-literal
is greater than †	A literal value to match; required match-literal
is less than or equal to†	A literal value to match; required match-literal
is less than†	A literal value to match; required match-literal
is one of†	A comma-separated list of literal values, at least one of which must be specified, but only one of which need match match-literal-1[,match-literal-n,...]
is between†	A range specified as start and end literal values; both must be specified; range is inclusive start-range-literal , end-range-literal
contains†	A string literal on which to perform pattern matching; required [FALSE TRUE,] 'pattern-literal' FALSE (default) means string must comply with Oracle LIKE operator syntax; TRUE means string must comply with Posix regular expression syntax
replace‡	A string literal to match and replace with a second string literal [FALSE TRUE,] 'pattern-literal' [, 'replacement-literal'] [, position-integer] [, occurrence-integer] FALSE (default) means string must comply with Oracle LIKE operator syntax; TRUE means string must comply with Posix regular expression syntax TRUE enables optional positional integer argument to indicate where within the column value to extract the string, and optional occurrence integer argument to indicate the position count to replace Mandatory pattern literal represents the string value to match If the replacement string literal is unspecified, replace the matched string literal with nothing

Operator	Operands
substring‡	<p>Extract specified segment of string value</p> <p>[FALSE TRUE,]position-integer[, length-integer][, 'pattern-literal' [, occurrence-integer]]</p> <p>FALSE (default) means string must comply with Oracle LIKE operator syntax; TRUE means string must comply with Posix regular expression syntax</p> <p>Mandatory positional integer argument indicates where to begin string extraction:</p> <ul style="list-style-type: none"> ■ If 0 or 1, returns all characters ■ If positive integer, starts extraction from beginning ■ If negative integer, starts extraction counting backwards from end <p>Optional length integer argument indicates character count starting at position integer</p> <p>pattern literal represents the value to match; optional if the first argument is FALSE; required if TRUE</p> <p>occurrence integer argument indicates character count to match; valid only if pattern literal is specified</p>

Notations are as follows:

- *–Enabled for value constraints, matching rules, and ignore rules
- †–Enabled for value constraints and ignore rules only
- ‡–Enabled for matching rules only

26.5.5 Understanding Rules by Example

These rule examples assume that you are in the process of creating or editing a template and are at the point where you have selected the configuration item in the tree on the left.

26.5.5.1 Matching Rule Examples

Suppose, when comparing the hardware of host configurations, you want, for matching purposes, to ignore case in respective vendor names. Here’s a simple rule to make the comparison case-insensitive.

1. In the **Rules for Matching** tab, click **New**.
2. Select **Vendor Name** in the drop-down list.
3. Select the table row and click the **Edit Rule** button in the toolbar to open the rule dialog.
 - Set **Operator** to `is-case-insensitive-equal-to`. As this operator takes no operands for a matching rule, you are done.
 - Click **OK**.

You want to compare WebLogic Servers, aligning on server name, where the names are different: `ManagedServer1` and `ManagedServer2`, for example. To ensure the comparison occurs, you need to fashion a match on server name.

1. In the **Rules for Matching Instances** tab, click **New**.
2. Select **Machine Name** in the drop-down list.

3. Select the table row and click the **Edit Rule** button in the toolbar to open the rule dialog.
 - Set **Operator** to `substring`.
 - Set **Operands** to `1, 13`.
 - Click **OK**.

Effectively, the rule says use the first 13 characters of the name (ManagedServer), thus excluding the qualifying integer.

4. Another way to achieve the same result:
 - Set **Operator** to `replace`.
 - Set **Operands** to `true, '*(\d*)', '\1'`.
 - Click **OK**.

This example uses a regular expression (TRUE) to resolve all characters prior to the qualifying integer.

For a more advanced example, consider a database instance comparison that requires a match on Datafiles filenames within a Tablespace, where filenames are of the form:

```
/u01/jblack_abc2d/oracle/dbs/dabc2/mgmt_ad4j.dbf
```

1. In the **Rules for Matching Instances** tab, click **New**.
2. Select **File Name** in the drop-down list.
3. Select the table row and click the **Edit Rule** button in the toolbar to open the rule dialog.
 - Set **Operator** to `replace`.
 - Set **Operands** to `true, '(/u01/)(.*) (oracle.* /dabc[0-9]+.*) (.*)', '\2\4'`.
 - Click **OK**.

Effectively, the rule says use a regular expression (TRUE) to construct a matching key from the value between `/u01/` and `oracle`, combined with what remains of the original filename after `dabc2 /`, or `jblack_abc2d/mgmt_ad4j.dbf`.

26.5.5.2 Ignore Rule Examples

Generally, you use ignore rules to ignore differences in collections that are row-oriented, as opposed to column-oriented. Custom Configuration snapshots, for example, are row-oriented data collections.

Say, for example, you wanted to ignore in Custom Configuration parsed data, any row where the property `Attribute` identifies an internal ID or checksum.

1. In the **Rules for Ignoring Instances** tab, click **New**.
2. Select **Attribute** in the drop-down list.
3. Select the table row and click the **Edit Rule** button in the toolbar to open the rule dialog.
 - Set **Operator** to `is one of`.
 - Set **Operands** to `'id', 'checksum'`.
 - Click **OK**.

The rule ensures that the comparison ignores any row in the collection data that contains either of the specified values.

Now consider an ignore rule that demonstrates how the comparison engine applies the logical operators AND and OR against the same configuration item type. In this example the objective is to ignore rows in Custom Configuration parsed data when any of three rule sets satisfies the following conditions:

Data Source = 'sqlnet.ora' AND **Attribute** = 'ADR_BASE'

OR

Data Source = 'tnsnames.ora' AND **Attribute** = 'HOST'

OR

Data Source = 'resources.xml' AND **Attribute** = 'authMechanismPreference'

Notice that the comparison engine applies the AND operator to rules within a set and the OR operator between rule sets. Rules for ignoring instances support inheritance; thus, in this case, the Data Source property is available in rules creation, as demonstrated in the example.

1. In the **Rules for Ignoring Instances** tab, click **New**.
2. Select **Data Source** in the drop-down list.
3. Select the table row and click the **Edit Rule** button in the toolbar to open the rule dialog.
 - Set **Operator** to is equal to.
 - Set **Operands** to 'sqlnet.ora'.
 - Click **OK**.
4. Click **New** and select **Attribute** in the drop-down list.
5. Select the table row and click the **Edit Rule** button in the toolbar to open the rule dialog.
 - Set **Operator** to is equal to.
 - Set **Operands** to 'ADR_BASE'.
 - Click **OK**.
6. Click **New Or** to insert a logical OR operator to signal the end of the first rule set.
7. Add two new rules where **Data Source** is equal to 'tnsnames.ora' and **Attribute** is equal to 'HOST'.
8. Click **New Or** to insert a logical OR operator to signal the end of the second rule set.
9. Add two new rules where **Data Source** is equal to 'resources.xml' and **Attribute** is equal to 'authMechanismPreference'.

The comparison ignores any row in the collection data that satisfies any of the three rule sets.

26.5.6 About Comparisons

Enterprise Configuration Management deals with the collection, storage, and monitoring of configuration data tied to managed entities within the enterprise. A host, for example, has configuration item types related to its hardware and software components—number of CPUs, memory, IO devices, OS platform and version, installed software products, and so forth.

Changes to configuration data invariably happen, typically because of common events like patches and upgrades. At some point a change to one component can affect the overall system in a negative way. Detecting the root cause becomes paramount.

The comparison tool enables you to compare configurations of a target with configurations of another target of the same type. The comparisons can be done on the current configuration or configurations previously saved (perhaps, for example, just before applying a patch or doing an upgrade).

Comparisons allow you to do the following:

- Ignore certain attributes during a comparison
- Notify key personnel when differences are detected
- Design and share comparison templates with other administrators
- Schedule a comparison to run on a recurring basis
- Compare complete target systems; match target system members automatically or manually
- Compare configuration file data as raw file content or in a parsed format

26.5.7 Understanding the Comparison Wizard

Comparisons are an important factor in managing the enterprise. The comparison wizard walks you through the process of setting up a comparison. Setting up a comparison involves five steps, six if you are comparing systems:

- Select the first configuration in the comparison (the one to compare against)
- Select additional configurations (the one or more configurations to compare to the first configuration)
- Select a comparison template to frame the comparison (or no template)
- When comparing systems, map system members in the first configuration to members of the other configurations
- Schedule the comparison job and set up e-mail notifications
- Review your work and submit the job

A follow-on step would be to review the results and drill down to differences details.

26.5.7.1 Selecting a Configuration to Compare Against

The first step in setting up a comparison is to select a configuration against which to compare one or more other configurations. When you open the Comparison Wizard (from the **Enterprise** menu, select **Configuration**, then select **Compare**), available configuration collections appear in a table at the bottom.

1. Choose between the latest and a saved configuration. You can "mix and match" in that you can compare latest to saved and vice versa. When you choose saved, filtering criteria on the right become active so that you can enter dates and a description.
2. Specify filtering criteria to narrow the search. Minimally, you would probably want to select a target type, and for a saved configuration, a before or after date. Click **Search**.
3. In the list of matching configurations that appears at the bottom of the page, select the one to be the benchmark and click **Next** or **Comparison Configurations** on the workflow train.

26.5.7.2 Selecting Configurations to Compare

The next step is to select one or more configurations to compare to the first configuration you selected.

1. Click **Add Configurations** to open the Search and Select Configurations dialog.
2. As for the first configuration, choose between latest and saved, and enter filtering criteria to narrow the search. Click **Search**.
3. In the results list, select one or more configurations (you can multiselect), then click **OK**.
4. Click **Next** or **Comparison Template** on the workflow train.

26.5.7.3 Selecting a Template to Use in the Comparison

Optionally, you can elect not to use a template (the default), in which case you can skip this step. You must use a template you select as is; that is, you cannot alter any settings for this particular comparison. If you want to change certain settings in a template, use the create-like feature to create a new template, based on an existing one.

Depending on the comparison target type, there may be a default template available. When done selecting a template, click **Next** or **Schedule and Notify** or **Mapping**, as appropriate, on the workflow train.

26.5.7.4 Mapping Members in a System Comparison

Mapping pertains exclusively to systems. It's a way to selectively indicate how members of respective systems should match up in a comparison.

Initially, the view displays a table of systems being compared to the first system, with no mapping details. Select a table row and the Mapping Overview displays the system target type hierarchy and the mappings that exist between the first and second target. These mappings are determined either by the target-matching rules defined for the template selected in the previous step, or by system-defined target-matching rules, if no template was chosen. If you are comparing multiple systems, select a different system target to see the mappings for that system.

Tip: The mapping display provides feedback on left-only and right-only match-ups in advance of actually running the comparison, giving you the opportunity to create matching rules in the template to address the issue.

You can choose to disregard members from the comparison by selecting the **Ignore** check box next to those member targets. This selection automatically ignores any child members as well. If you select the check box in the table header, all members are ignored.

Template- or system-based mappings may not account for all situations. Click the **Create Mapping** button to manually map members in the first system to members in the second system.

The pop-up dialog displays tree hierarchies of the respective system targets. When you select a member in the first system, check boxes designate suitable target members in the second system. Select one or more members to which to map the member in the first system. Note that the mapping automatically includes children of a mapped member. When you select another member in the first system, the mappings you just set disappear from view, but persist. When you are done, click **OK** to confirm the manual mappings and close the dialog.

The Mapping Overview hierarchy now includes the manual mappings you just created, as denoted by the manually mapped icon in the Status column. Other icons denote system mapped, which covers both system- and template-based mappings; ignored members, and left- or right-only members. Hover the mouse pointer over the icon in the Status column to interpret the icon.

To remove any mappings that were manually created, click the **Remove Mapping** button. The pop-up dialog displays tree hierarchies of the respective system targets, showing any manual mappings that were created. Select the check box in the Remove column for any manual mapping you want to undo. Note that removal of a member mapping automatically removes all child mappings.

When you are done with mapping, click Next or Schedule and Notify on the workflow train.

26.5.7.5 Scheduling the Comparison and Creating a Notification List

On the Schedule and Notify page, you schedule the comparison to run as a background job. The comparison can be one-time-only or run on a recurring basis. You can run the comparison immediately or at some later date. This also is where you supply e-mail addresses to which to send differences alerts.

Note: If you schedule a recurring job, you can subsequently change the job-related settings when viewing the results on the Jobs page. Click the **Edit** button, then go to the **Schedule** tab.

1. The comparison job must have a name. Although the system supplies a default name that identifies it by date and time as a configuration comparison, you may want to enter a meaningful name for the job.
2. Specify the job schedule:
 - **If not now, when.** Click **Later** to activate the calendar widget where you can select a date and time.
 - **How often.** Select report frequency in the drop-down list. Default is one-time-only.
 - **Wait how long.** If the job fails to run as scheduled, cancel within a specified time frame.
 - **Keep going.** Maintain the job schedule for the specified period.
3. Enter the e-mail addresses of those who are to be notified when the comparison detects a difference. Use a comma to separate addresses. Remember that the properties for which differences are alerted were specifically selected in the comparison template.

As logged-in user and originator of the comparison, you must have properly set up your account for sending notifications via the Enterprise Manager Notification System (from the **Setup** menu, select **Notifications**, then select **Notification Methods** on the console home page). The settings for Identify Sender As and Sender's E-mail Address will appear on e-mail generated as a result of differences detected by the comparison job.

4. Click **Next** or **Review and Submit** on the workflow train.

26.5.7.6 Reviewing the Comparison Parameters and Submitting the Job

Review the comparison parameters before submitting the job:

- Is the benchmark configuration, that is, the first one, correct?
- Are the configurations you are comparing against the benchmark correct?
- Are you using the template you want?
- Is the job name suitable?
- Is the job scheduling as intended?
- Have you entered properly formatted e-mail addresses for differences alerts?

If you need to change anything, go back to the appropriate page; otherwise, click **Submit** to schedule the comparison job.

The Jobs page opens, showing a summary of the submitted job. Eventually the Jobs page reveals the results of the comparison; that is, whether the comparison detected differences or found the configurations to be the same. In either case (different or the same), the reported result is a link to the details of the comparison, although presumably different is the more interesting result. A separate entry appears for each compared configuration. In other words, if configurations B and C are being compared to A, there is a result for A compared to B, and a result for A compared to C.

26.5.8 Working with Comparison Results

This section covers comparison results from the following perspectives:

- [About Comparisons and Job Activity](#)
- [About System Comparison Results](#)
- [About Standard Target Comparison Results](#)
- [Synchronizing Configuration Files](#)

26.5.8.1 About Comparisons and Job Activity

Comparisons run as scheduled jobs. Part of the process of setting up a comparison is to define the schedule: run once-only or on a recurring basis; run immediately or at some later time; retry after failure; and so forth. Given the permutations, you can have many jobs to keep track of.

To view comparison job activity, from the **Enterprise** menu, select **Configuration**, then select **Comparison Job Activity**.

Note that the comparison job activity page also affords the opportunity to resubmit comparisons already run; that is, you do not have to go through the entire comparison workflow to run a subsequent execution of the same comparison.

View a list of all current and past comparisons. Use search criteria to filter the list of comparison jobs. For example, show all failed comparisons started over the past 24 hours; or, show all successful comparisons involving hosts started over the past 31 days. The jobs engine purges comparison jobs older than 31 days.

Select a table row and click **View Result** to go to the Jobs page that reports the comparison result. From there you can drill down to results details. The job name is a hyperlink that takes you to the same place. Use the bread crumb on the Jobs page to navigate back to the list. The comparison jobs you can view beyond your own depend on your role and access level granted.

Select a table row and click **Resubmit Comparison Now** to run a new submission of a previously executed comparison, characterized by the following.

- As this is a new job, a date and time stamp distinguishes it from its predecessor.

- The job is scheduled to execute immediately.
- The job will execute only once.

An informational message confirms the job, which appears as a new row in the table.

If you are the job owner or otherwise have the proper access level, you can perform list maintenance by deleting comparison jobs that no longer have relevance. This has the effect of purging the comparison results as well.

26.5.8.2 About System Comparison Results

Results of a system comparison appear when the scheduled comparison job completes and you click the Different link on the Jobs page. You can of course view results by clicking the Same link, but viewing and resolving differences is typically the objective of comparisons.

The region at the top summarizes the comparison and job details. The region at the bottom displays a system comparison results summary table. As system comparison results can span a large number of rows, you can filter the results to curtail the display. Click the Search down arrow to expose the filtering criteria. The search results highlight the members that satisfy the criteria and show ancestors up to the root.

The table displays a hierarchy of system and member target types where:

- The Target Type column displays the system and member tree hierarchy.
- The Result column shows comparison results based on the mappings established as part of comparison setup. A boxed 1 (left only) or 2 (right only) means there was nothing to compare to the first or second member target, respectively. Note that if the parent target configurations are the same, but one or the other parent has child members marked as left only or right only, the parents are marked as different.
- To resolve unmatched members, rerun the comparison in the wizard, this time ensuring in the mapping step that the left and right member pairs appear in the mapped members table. Select an appropriate system comparison template with target matching rules defined, such that these members are mapped, or map the pairs manually.
- If, for the purposes of a system comparison, you prefer not to compare members of a given target type (for example, trying to diagnose a system setup issue where differences at the member level would be irrelevant), select the **Ignore** check box in the mapping step to bypass a given member type.
- Click the Different link to see the differences between member targets, as displayed on the standard comparison results page. Use the bread crumb link at the top of the details page to return to the system comparison results page.

When the Results column displays both an equal and a not equal icon, it indicates equality at the parent level, but a difference in some member.

26.5.8.3 About Standard Target Comparison Results

Difference details display when you click the Different link in the comparison results view on the Jobs page. The details view summarizes the comparison and job details. You may want to collapse these regions to provide more page real estate for the difference details.

Difference details break down as follows:

- The left pane displays a hierarchy of configuration items for the target type being compared, and, if applicable, custom configurations. Refine the scope of comparison results as follows:
 - Select the **Show Differences Only** check box to eliminate the "noise" of same and ignored results.
 - Select the **Show Ignored** check box to display properties the comparison template ignores. Key properties and properties that are the same or different display by default. This option is disabled if you selected **Show Differences Only** in the left pane.
- The display on the right depends on the selection on the left.
 - Should the selection on the left have up to six key properties, but only one value property, the table on the right displays all key columns first, and then the value column, where the respective value appears for the first and second configuration. The key columns do not appear twice as the values have to be the same for the rows to be compared in the first place.

Use the filter feature above the right table to search for configuration items where the key or value columns match.
 - If the selection on the left has more than one value property, the display on the right shows a top table that contains rows of select (key) configuration properties and a bottom table that contains rows of all configuration properties, including both key and value properties.

Select a row in the top table to move its configuration property to the top row of the bottom table.
 - For single-row configuration item types, that is, item types that have no key properties, but many attribute properties, the right pane displays the compared property values of the first and second configurations in a single table, where the first column of the table lists the property names.
 - Select a configuration specification on the left to display tables on the right where the top table contains the configuration files with differences and the bottom table contains rows of configuration properties and values. Notice in this view that you can synchronize the file differences (**Enable File Synchronization**). For details on file synchronization, see [Section 26.5.8.4](#).
 - Select a custom configuration file on the left to display file contents on the right. File contents that include property values for the compared configurations display both in raw and parsed form on separate tabs.

The icons that appear in this view are mostly intuitive: equal–same, not equal–different. The key icon denotes the key properties of the configuration item type. An indication of Out of Range means that the property value failed a value constraint set on the property. A boxed 1 (left only) or 2 (right only) means that the comparison did not find a matching item to compare to the first or second configuration, respectively. When this is the case, use the link that appears below the Comparison Details label to open the template in edit mode so that you can invoke a rule to create a match, and then rerun the comparison.

Configuration Key Properties

You might wonder about the column names that appear in the top table on the right. These columns represent configuration item type key properties. If the configuration item type does not have declared key properties, the comparison engine takes the top four properties in the CI type database table to serve as key stand-ins for purposes of

matching up configurations. The comparison engine upholds the same precedence (top four properties in the database table) if for some reason the comparison is set up to ignore key properties (not recommended).

26.5.8.4 Synchronizing Configuration Files

Use this feature to perform on-demand file synchronization when a comparison of file-based configurations returns differences. Often, this involves custom configurations that users create. See [Section 26.6, "Overview of Custom Configurations and Collections,"](#) for information on custom configurations.

Note: This feature is available only for file-based configurations. Differences resulting from comparisons of command-based or SQL query-based custom configurations cannot be synchronized.

1. When viewing comparison results differences, select the configuration specification in the tree on the left.
2. The **Enable File Synchronization** check box now appears. Select it.
3. A drop-down list now appears next to the check box. Select the direction of the update; that is, change the second configuration to match the first, or vice versa.
4. In the new Synchronize File column that appears, select which files to update. You can select multiple files, indicating that you'll be updating all of them in the same direction.
5. Optionally, use the Preview feature to view the effect of the update on a file-by-file basis. Click the eyeglasses icon to view the file before and after the update in raw format.
6. When satisfied with the results, click the **Synchronize Files** button.
7. Complete the dialog that opens as follows:
 - Specify the login credentials as necessary. You must have login access to the target destination and write permission on the directory or directories to be updated.
 - Select the appropriate radio button to indicate a destination directory. In either case (original or alternate), you must have write permission on the directory.
 - Select the appropriate radio button for how to proceed on conflict. The comparison is performed using data from the repository. A conflict arises when the file to be updated has changed on the target and is different from the data used for the comparison. Indicate what you want to do in this case—proceed or stop.
 - Note that irrespective of the selection for destination directory (original or alternate), the conflict check is always performed against files in the original directory.
 - Indicate the desired backup options (both are selected by default when the update target is the original directory):
 - Mark the appropriate check box if you want to save a snapshot of the configuration to be updated prior to synchronizing (give it a descriptive name so you can easily retrieve the file from saved configurations; defaults to a generic name—CCS Synchronization Saved Snapshot—which applies even if you blank the field).

- Mark the appropriate check box if you want to make a backup copy of the configuration file before it's updated. Browse to a directory on which you have write permission.

These are not mutually exclusive options. With the former, you are saving time-stamped collection data in the OMS repository; whereas, with the latter, you are storing a copy of a file in a file system.

- If desired, perform an on-demand collection refresh of the destination target's configuration data immediately after file synchronization. This way, if you rerun the comparison or view the configuration in the Configuration Browser, the effects of the update will be visible. You can also run a manual refresh at any time, or wait for the next scheduled collection.

The check box is selected by default when the original destination directory is the update target. The check box is disabled if you specified an alternate directory, as there would be nothing to refresh in this case.

- Click **OK**.
- Click **Yes** to confirm the file update.

Use the link in the Confirmation area to track the synchronization job. When the job completes, you can rerun the comparison to verify the update, assuming you requested a refresh. You can also open the custom configuration in the Configuration Browser and confirm the update there.

Not All Configuration Files Can Be Synchronized

You may notice in the comparison results differences view that some files, though different, cannot be selected for synchronization (their check boxes are disabled). There are several possible reasons, including:

- The destination file is nonwritable.
- There is no source file.
- During the custom configuration definition, the file was associated with a parser that does not support a process called reverse transform, which is, effectively, the ability to return the parsed form of a file to a syntax tree structure that can then be rendered back into a physical representation. Not all parsers support reverse transform.

26.6 Overview of Custom Configurations and Collections

Custom configurations provide a way to identify files and other configuration data that Cloud Control does not already collect. These customized configurations can be collected on well-known target types or on a target type introduced as part of the custom configuration definition. A set of custom configurations called blueprints are available for download from Oracle. They are called blueprints because they lay out precisely the files and data to collect for a given platform such as Apache Tomcat.

A typical life cycle of a custom configuration might be as follows:

- Create a custom configuration and deploy it to several targets.
- Assess its effectiveness over time.
- Modify and fine-tune the specification and redeploy, perhaps across a wider spectrum.
- Undeploy and delete the specification if no longer pertinent.

This section covers the following topics:

- [Working with Custom Configurations](#)
- [About Custom Configurations and Deployment](#)
- [Extending Configuration Data Collections](#)
- [Using Custom Configurations as Blueprints](#)

26.6.1 Working with Custom Configurations

This section describes how to create, edit, and otherwise manage custom configurations.

26.6.1.1 Creating or Editing a Custom Configuration

Use the instructions below to create, create like, or edit a custom configuration.

Given appropriate privileges, you can edit a custom configuration and save the edited version, in which case, the version number increases. You might also edit and save as a draft, or edit a draft for publishing. Note that when you edit a custom configuration, you cannot change the target type, as this would cause the underlying metadata to be incompatible with existing deployments of the custom configuration.

See [Section 26.6.1.8](#) for information on privileges required to perform various actions on custom configurations.

Note: When you edit a deployed custom configuration, it is automatically redeployed upon saving. This does not apply to saving as draft.

1. In the Custom Configurations library, click the **Create** button; or, select an existing specification in the library and click **Create Like** or **Edit**.
2. On the Create Custom Configuration page, enter a name for the custom configuration and an optional description. The create like action requires minimally that you rename the specification.
3. Select a target type. If no currently defined target type satisfies your requirements, click the **Create Custom Target Type** button to the right of the target type drop-down list. Type a name and click **OK**. The new type now appears in the drop-down list of target types.

To create a new target type, ensure that the administrator has installed a software library (from the **Setup** menu, select **Provisioning and Patching**, then select **Software Library**). This must be done once, after Cloud Control installation.

4. Optionally, set up a sample target. A sample target resides on the host from which you intend to collect configuration data. If you do not set up a sample target, you cannot browse the file system or use the preview feature in entering your specifications. You can select an existing target instance as a sample, or add a new one. Typically, you would add a new target instance to match a custom target type added in Step 4.
 - To select an existing target instance, click the appropriate link. A dialog opens containing known instances of the target type. Use the filtering criteria as necessary to locate the instance you want, then click **Select**.

- To add a new target instance, click the appropriate link. As instructed in the dialog that opens, you must first select a Management Agent to monitor the target you are adding. Next, click **Add Target**. In the dialog that opens, provide target properties appropriate to the instance target type. Minimally, provide values for required properties (denoted by an asterisk). For a new target instance that matches a custom target type, the pertinent target property is the path to install home, as this is the likely location of configuration files relevant to the custom target type.
- 5. See [Section 26.6.1.2](#) for instructions on how to complete the Files & Commands tab.
- 6. See [Section 26.6.1.3](#) for instructions on how to complete the SQL tab.
- 7. After you complete the specification definition and have mapped credentials to the target type, use the preview feature to validate your entries, in particular, to ensure the parsed view is what you expect.
- 8. Save the new or edited specification. Remember that custom configurations are in the public domain. Use the save-as-draft feature to keep the specification private while you test and refine it. See [Section 26.6.1.7](#) for more information on the ramifications of save actions.

If you are editing a draft, the buttons change as follows:

- **Publish** implies that you are making the draft public.
- **Save** implies that you are creating the next version of the draft.

When done, you can begin collecting configuration data by deploying the custom configuration to target instances. See [Section 26.6.2](#) for more information.

26.6.1.2 Using the Files & Commands Tab

Create file and command specifications as follows:

1. Click the search icon to browse to a default base directory location. This is where the configuration files reside, or where the commands you specify are to execute.

Click the **Use Property** button to open a dialog where you can select a target property to include as part of the directory path. These properties serve as variables, denoted by curly braces, to be substituted with actual values at runtime. You can type additional text in the box to supplement your selection. So, for example, you might select OracleHome and append a directory—`{OracleHome}/config`—to collect files on the target located in the config subdirectory under the Oracle Home path. Note that the target type definition determines available target properties. User-defined properties do not appear in the list, as they are not available at the Management Agent.
2. Click **Advanced Settings** to specify the following:
 - An alternate base directory for the sample target.
 - The encoding to use in collecting the data at the Management Agent. Configuration data is stored in UTF-8 format in the repository. Oracle Default means use UTF-8 for XML files and the locale encoding of the target for all other file types; Target Locale means store all file types including XML in the locale encoding of the target; otherwise, select an encoding from the drop-down list. Selecting directly from the list automatically selects the accompanying radio button.
 - Whether to use the Management Agent credentials (file specification only) or some other predefined credential set to access data on the target. If the

customized credential set does not appear in the drop-down list, click **Create** to identify the credential set to use. Note that you must then specify the credentials that map to the credential set name you create. If you don't know a mapped name, you can specify a credential set when you open the Remote File Browser to add files as described in Step 3. See [Section 26.6.1.4](#) for more information.

3. Click **Add** and select file or command as the specification type.

For a **file specification**, enter a file name in the space provided or browse the base directory to select a file on the target. Use of wildcards (* and **) is allowed, where ** indicates 0 or more subdirectories. In using wildcards (and as a general caveat), ensure that collections do not result in too many (or too large) files, and that the files collected be configuration-related, that is, files under administrative control that change relatively rarely, so as not to overload Cloud Control.

For a **command specification**, enter command syntax in the space provided or browse the base directory to a script. You must assign a unique alias to the command. The alias you assign appears in the Configuration Browser as a link when viewing the custom configuration hierarchy. When you click the link, it opens the command specification in the tab on the right. The same caveats as mentioned for files apply to command output; that is, that their results are constrained in number and size, and to configuration-related data.

Select a parser to convert the configuration file or command output into a standard format for storing in the repository. There is no default. If you do not specify a parser, only the raw data format is stored and available for viewing. See [Section 26.7.1](#) for more information.

Optional. Specify post-parser rules to align tree nodes. See [Section 26.6.1.5](#) for information on entering rules.

4. Repeat Step 3 to specify additional files or commands.

Return to [Section 26.6.1.1](#) and resume with 7.

26.6.1.3 Using the SQL Tab

Create SQL query specifications as follows:

1. Select credentials to use to connect to the database. If the customized credential set does not appear in the drop-down list, click **Create** to identify the credential set to use. Note that you must then specify the credentials that map to the credential set name you create (see [Section 26.6.1.4](#)). Custom configurations only support database credentials with NORMAL roles, not those with SYSDBA, SYSOPER, or other roles.
2. Specify a JDBC connection to an Oracle database from which to extract data via an SQL query. The connection string can be either a URL or an abstraction of database target properties. It cannot be a combination of the two; that is, partial URL and some target properties.

The URL must contain the name of the target database host, applicable port number, and the Oracle Service name (SID); for example,
mydatabase.us.oracle.com:1521:ORCL.

If you want to use target properties, leave the field blank. At runtime the application will substitute values for these target properties—{MachineName}{Port}{SID}—to make the connection.

3. Click **Add** and type or paste a SQL query in the provided text box. Ensure that the query is sufficiently selective to return only pertinent configuration-related data of manageable size and scope.

You must assign a unique alias to the query. The alias you assign appears in the Configuration Browser as a link when viewing the custom configuration hierarchy. When you click the link, it opens the SQL query in the tab on the right.

Database Query Parser should be preselected in the drop-down list.

Optional. Specify post-parser rules to align tree nodes. See [Section 26.6.1.5](#) for information on entering rules.

4. Repeat Step 3 to specify additional SQL queries.

Return to [Section 26.6.1.1](#) and resume with Step 7.

26.6.1.4 Setting Up Credentials

If you create a credential set while creating a custom configuration, you have to specify the credentials that make up the credential set. To do this, you have to return to the Custom Configurations library and proceed as follows:

1. From the **Setup** menu (top right of the page next to the Help menu), select **Security**, then select **Monitoring Credentials**.
2. Select the applicable target type in the table and click **Manage Monitoring Credentials**.
3. Select the row with the credential set name you created during the custom configuration definition for the given target type and click **Set Credentials**.
4. Enter the username and password for the credential set and click **Save** (or **Test and Save** for database credentials).
5. Return to the Files & Commands tab ([Section 26.6.1.2](#)) or SQL tab ([Section 26.6.1.3](#)) description.

26.6.1.5 Setting Up Rules

Use rules to differentiate nodes in the parsed representation that have the same name. This is particularly important in comparisons and change history when trying to match nodes in the parsed tree, or when expressing SQL queries to verify compliance. Rules resolve to an identifier that is appended in square brackets to node text in the tree as a way of uniquely identifying the node. An operation such as a comparison will then use the combination of node text and bracketed identifier for evaluation purposes.

A rule consists of a condition and an expression, both of which must be valid XPath expressions. The condition resolves to a node that requires the identifier. The expression resolves to a string computation for the identifier. You can use a special case **SKIP** expression to bypass the node specified in the condition; this is a convenient way to eliminate "noise." In other words, for purposes of comparison, ignore the node the condition resolves to.

Some parsers have default parser rules already defined. They execute automatically on the parsed representation. You can elect to use a subset of default rules, edit them, or override them with custom rules that you define.

The number in the **Rules** column is significant. Initially, the number is zero (0). A whole number greater than zero indicates the number of custom rules defined. Zero also appears for a parser that has default parser rules. So the appearance of a whole

number in the column stipulates an override of default parser rules, if any, with the custom rules the number represents.

Set up rules as follows:

1. Click the **Parser Rules** button. The Edit Parser Rules page displays.
2. To define a custom rule, click **Add**. In the table row that appears, enter a condition and an expression as valid XPath expressions.

You can define multiple rules; they are applied to the parsed content in the order specified. Click **Return** when you are done.

Select a table row to delete a custom rule.

3. To manipulate default rules, click **Add Default Rules**.

Rules appear in table rows, provided the parser you selected has default parser rules. Edit and delete default rules as appropriate to your purposes. Remember that you are working with a copy of these rules; the originals remain safely intact.

Note that if you delete all rules, you are merely removing the copies you imported. Default parser rules will still fire unless overridden by custom rules.

For examples of rules, see [Section 26.7.6](#).

Return to the Files & Commands tab ([Section 26.6.1.2](#)) or SQL tab ([Section 26.6.1.3](#)) description.

26.6.1.6 Managing Custom Configurations

In addition to creating and editing custom configurations, you manage them by doing the following:

- View the selected specification (read-only)
- Synchronize the selected specification with facets in the Compliance Library for real-time facet monitoring
- Share custom configurations by exporting them in XML file format and importing them from the local file system
- Delete the selected specification (requires the proper permissions)

Viewing a Custom Configuration

You can view a custom configuration in read-only mode to get an idea of the make-up of a specification. Perhaps, for example, to see if it is a likely candidate on which to base a new specification.

1. In the Custom Configurations library, select the specification table row and click **View Details**.
2. Peruse the settings and rules on the various tabs.

Enabling Facet Synchronization

You can synchronize a custom configuration specification with real-time monitoring facets to monitor real-time changes to the configuration files and queries that make up the custom configuration. Real-time monitoring enables you to know such things as when files and database settings change, who made the change, whether observations were automatically reconciled, whether the actions observed were authorized, and so forth.

When you synchronize custom configurations with real-time monitoring facets, future changes to custom configurations automatically propagate to corresponding facets, which means configurations are not only collected, compared, tracked, and so forth, but also are monitored for authorized real-time changes. Note that to associate a custom configuration with a facet and to subsequently edit a custom configuration synchronized with a facet requires the additional role of EM_COMPLIANCE_DESIGNER.

1. In the Custom Configurations library, select the specification table row and click **Enable Facet Synchronization**.
2. The **Facet Synchronization** column displays a **Use Facet** link in the custom configuration table row. Click the link to go to the **Real-time Monitoring Facets** tab in the Compliance Library where you can manage the synchronization of facets with the custom configuration.

Exporting a Custom Configuration

You can export a custom configuration as an XML file that can subsequently be imported into the same or another system.

1. In the Custom Configurations library, select the specification table row and click **Export**.
2. Browse to a file system location where you want to save the specification as an XML file. The saved file takes the name of the custom configuration by default.

Importing a Custom Configuration

Given appropriate privileges, you can import a custom configuration that was previously exported as an XML file.

1. In the Custom Configurations library, select the specification table row and click **Import**.
2. Browse to the file location. Select the file and click the **Import** button on the dialog.
The imported specification appears in the Custom Configurations library.

Deleting a Custom Configuration

You must be the owner or otherwise have sufficient privileges to delete a custom configuration. Note that there are dependencies that potentially impact deletion, including deployments, job schedules, existing collections, and so forth.

1. In the Custom Configurations library, select the specification table row and click **Delete**.
2. The system validates permissions and otherwise checks for dependencies that might prevent the deletion, although some dependencies cannot be verified until a job submission involving the custom configuration.

26.6.1.7 About Custom Configurations and Versioning

When you create a custom configuration, you have options to save or save as draft. A normal save action makes the specification publicly available to the general user community. A save as draft action keeps the specification private to you. How you use these actions when creating and editing specifications influences the mechanics of versioning. Consider the following scenarios:

- You create and save a custom configuration; this is public version 1. You subsequently edit public1 and save as a draft; this becomes draft1. Public1 is still generally available. You edit draft1 and publish; this becomes public2. Note that in

parallel, someone else with the proper permissions can also edit public1 and save as a draft to create version 1 of draft2.

- You create and save a custom configuration as a draft; this is version1 of draft1. You edit and save again; this becomes version 2 of draft1. Repeat the edit-and-save operation; this becomes version 3 of draft1. Edit version 3 of draft1 and publish; this becomes public version 1.

26.6.1.8 About Custom Configurations and Privileges

Working with custom configurations requires privileges specific to the given operation you want to perform.

Operation	Required Privilege (Role)
Create new target type	EM_PLUGIN_OMS_ADMIN To create a new target type, ensure that the administrator has installed a software library (from the Setup menu, select Provisioning and Patching , then select Software Library). This must be done once, after Cloud Control installation.
Create new target instance	EM_PLUGIN_AGENT_ADMIN
Create or import custom configuration	"Manage custom configurations owned by user" (or the more powerful "Manage custom configurations owned by any user")
Associate custom configuration with an auto-synchronized real-time monitoring facet	EM_COMPLIANCE_DESIGNER
Edit or delete custom configuration	Differs, depending on the specific activity within the realm of editing: <ul style="list-style-type: none"> ■ Custom configuration owner requires "Manage custom configurations owned by user"; nonowner requires "Manage custom configurations owned by any user" ■ Schedule redeployment jobs for already deployed targets requires "Create" privilege for Job System resource type ■ For custom configurations associated with real-time monitoring facet, EM_COMPLIANCE_DESIGNER
Deploy or undeploy custom configuration on a target	"Manage target metrics" privilege on the target instance; "Create" privilege for Job System resource type (to schedule deployment/undeployment); EM_PLUGIN_AGENT_ADMIN (to deploy a plug-in to a Management Agent)
Create a new credential set	Superuser
View custom configuration definition	None
View custom configuration collected data	Regular "target instance view" privilege

Note that editing an imported custom configuration may be restricted to edits that do not change the version, depending on options set during export. One such permissible edit would be to credential set information.

26.6.2 About Custom Configurations and Deployment

Deployment of a custom configuration means to direct the specification to a target where a monitoring Management Agent will collect configuration data based on the

specification's definition. A custom configuration can be deployed to multiple targets. You must have sufficient privileges to deploy and undeploy custom configurations.

Manage deployments by performing the following actions:

- [Deploying and Undeploying Custom Configurations](#)
- [Editing a Deployment](#)
- [Viewing a Configuration Collection](#)

26.6.2.1 Deploying and Undeploying Custom Configurations

Deployment of a custom configuration means to direct the specification to a target where a monitoring Management Agent will collect configuration data based on the specification's definition. A custom configuration can be deployed to multiple targets. You must have sufficient privileges to deploy and undeploy custom configurations.

To deploy a custom configuration:

1. In the Custom Configurations library, select the specification table row and click **Deploy**.
2. On the Deployments page, click **Add**. In the dialog that opens, search for and select targets of the specified target type where you want to deploy the custom configuration.
3. When you close the dialog (click **Select**), a new column appears denoting a pending action of **Deploy** and the status becomes **Selected for deployment**.
4. Proceed as follows:
 - Click **Apply** to confirm the action while remaining on the Deployments page. The action column disappears, and the status becomes **Deployment job in progress**.
 - Click **OK** to schedule the deployment and return to the library.
 - Click **Cancel** to void the request and return to the library.
5. Click **Refresh Status** on the Deployments page to confirm a successful outcome.

If you update a deployed custom configuration, redeployment occurs automatically.

To undeploy a custom configuration:

1. Select the deployment in the table.
2. Click **Remove**. A new column appears denoting a pending action of **Undeploy**; status remains **Deployed**.
3. Proceed as follows:
 - Click **Apply** to confirm the action while remaining on the Deployments page. The action column disappears, and the status becomes **Undeployment job in progress**.
 - Click **OK** to schedule the undeployment and return to the library.
 - Click **Cancel** to void the request and return to the library.
4. Click **Refresh Status** on the Deployments page to confirm a successful outcome.

When viewing custom configurations in the library, a green check mark in the Deployments column denotes a currently deployed custom configuration. Click the check mark to open the Deployments page.

26.6.2.2 Editing a Deployment

To edit a deployment:

1. In the Custom Configurations library, locate the appropriate table row and click the deployments link.
2. On the Deployments page, select the deployment in the table and click **Edit**.
3. The type of custom configuration, that is, file/command-based or SQL-based, determines the make-up of the dialog that opens. Specify a base directory to override the default base directory currently in effect, or change the JDBC URL, as appropriate.
4. Proceed as follows:
 - Click **Apply** to confirm the action while remaining on the Deployments page. The action column disappears, and the status becomes **Redeployment job in progress**.
 - Click **OK** to schedule the redeployment and return to the library.
 - Click **Cancel** to void the request and return to the library.
5. Click **Refresh Status** on the Deployments page to confirm a successful outcome.

Note that the edit applies to the deployment of the specification; it does change the custom configuration definition.

26.6.2.3 Viewing a Configuration Collection

You must have sufficient privileges to view a custom configuration's collected data.

1. In the Custom Configurations library, locate the appropriate table row and click the deployments link.
2. On the Deployments page, select the deployment in the table and click **View Configuration**.
3. In the Configuration Browser popup window, peruse details of the custom configuration by selecting nodes in the tree hierarchy on the left:
 - The root node represents the target instance being monitored. The right pane displays target properties and immediate relationships.
 - The next level down in the tree represents a template for the specification. The right pane displays specification details such as configurations being collected and the base directory from which they are collected.
 - The remaining leaf nodes in the tree represent the configuration data collected. The right pane displays the configuration data in both parsed and raw format.

You can also view the collected data from the target home page: from the target type menu, select **Configuration**, then select **Last Collected**.

26.6.3 Extending Configuration Data Collections

There are two options available to extend configuration data collections using a custom configuration specification:

- Add additional collection items to an existing target type
- Add a custom target type with new collection items

26.6.3.1 Extending Existing Target Collections

The instructions below describe how to extend the configuration data Cloud Control collects for an existing target type. The listener target type, for example, does not collect the `sqlnet.ora` file out of box. To extend the listener data collection to include this item, take the following steps:

1. From the **Enterprise** menu, select **Configuration**, then select **Custom**.
2. In the Custom Configurations library, click the **Create** button.
3. Give the custom configuration an appropriate name and select **Listener** as the target type.
4. Click **Select Target Instance** to choose a listener instance that is already deployed, so you can browse to the file location.
5. Set the **Default Base Directory** to **OracleHome**.
6. You are now ready to build the collection data specifications. Click **Add**, then click the search icon to log in to the remote file browser. Set the credentials appropriately.
7. In the Oracle home directory of the listener instance, browse to the `network/admin` subdirectory and select the `sqlnet.ora` file. Add it to the selection table and click **OK**.
8. With the file added to the **Files & Commands** tab, select an appropriate parser from the drop-down list, in this case, the Oracle ORA parser. Click **Preview** if you want to see the file attributes in parsed and raw form as it will appear in the collected data.

Click **Save** to complete creation of the custom configuration.

9. In the Custom Configuration library, select the new custom configuration and click **Deploy**.
10. On the Manage Deployments page, click **Add**. In the dialog that opens, select the targets where you want to deploy the custom configuration.
11. When the status displays submitted, click **Apply**. Refresh the view until status is successful, then click **Save**.
12. To verify the added data collection, go to the target instance home page. From the **Oracle Listener** menu, select **Configuration**, then select **Latest Collected**.

The Configuration Browser should display the custom configuration in the tree structure on the left, where you can drill down the directory structure to display the parsed and raw forms of the `sqlnet.ora` attributes and values on the right.

Use this description as a template for extending existing configuration data collections.

26.6.3.2 Adding New Target Data Collections

The instructions below describe how to extend the configuration data Cloud Control collects by adding a new target type. The example assumes to collect data for a custom Apache web server target type.

1. From the **Enterprise** menu, select **Configuration**, then select **Custom**.
2. In the Custom Configurations library, click the **Create** button.
3. Enter a target name, `MyApache`, for example.
4. Click the **Create Custom Target Type** button. In the dialog that opens, enter a target type name, `MyApache`, for example. Click **OK**.

After a while, the dialog closes and the new target type name appears in the **Target Type** field. Note also that the `{INSTALL_LOCATION}` variable populates the **Default Base Directory** field.

5. As this is a new target type, there is no target instance to select, so click **Add Target Instance**.
6. As the text says, you have to first select a Management Agent. Click the search icon to open the selector dialog. To simplify the process in the example, the objective is to select a Management Agent on a host where the application (Apache Tomcat) already resides. Choose the Management Agent and click **Select** to close the dialog, then click **Add Target**.
7. In the target properties dialog that opens, enter the name (MyApache) and set the install home path to the start location of the application (Apache Tomcat) on the Management Agent. Click **OK** to deploy a new target type plug-in on the Management Agent. When you get the confirmation of deployment, click **OK**.
8. You are now ready to build the collection data specifications. Click **Add**, then click the search icon to log in to the remote file browser. Set the credentials appropriately.
9. In the Apache install home on the Management Agent, browse to the `conf` directory and select the `httpd1.conf` file. Add it to the selection table and click **OK**.
10. With the file added to the **Files & Commands** tab, select an appropriate parser from the drop-down list, in this case, the Apache HTTPD parser. Click **Preview** if you want to see the file attributes in parsed and raw form as it will appear in the collected data.

Click **Save** to complete creation of the custom configuration.

11. In the Custom Configuration library, select the new custom configuration and click **Deploy**.
12. On the Manage Deployments page, click **Add**. In the dialog that opens, select the targets where you want to deploy the custom configuration, for example, the host on which the custom configuration was based.
13. When the status displays submitted, click **Apply**. Refresh the view until status is successful, then click **Save**.
14. To verify the new data collection, do an all targets search and locate the custom target type under the **Others** category on the left and click it to display all deployments of that type on the right.
15. Click a target instance (MyApache) in the deployments list on the right. The Configuration Browser should display the custom configuration in the tree structure on the left, where you can drill down the directory structure to display the parsed and raw forms of the `httpd1.conf` attributes and values on the right.

Use this description as a template for extending configuration data collections through custom target types.

26.6.4 Using Custom Configurations as Blueprints

Specially formed custom configurations called blueprints are available for download from Oracle. They are called blueprints because they lay out precisely the files and data to collect for a given platform. Platform support currently includes:

- Apache Tomcat

- Apache Web Server
- GlassFish
- iPlanet
- JBoss
- JRun
- Tuxedo

You can download these blueprints, also called configuration extensions, from the Configuration Management Best Practice Center, where you can also check for new platform support.

26.7 Overview of Parsers

A Parser takes raw configuration data and parses it into a nested attribute structure. This structure is a tree hierarchy where nodes are containers and leaves are name value pairs of attributes, or properties.

Custom configurations include a host of out-of-box parsers. Each parser consists of a base parser and parser parameters. Some parsers also contain post-parsing rules. A base parser essentially is a category of parser capable of parsing data of a particular format. Parser parameters provide a way to tailor the base format to accommodate variations in data formatting. Post-parsing rules are a mechanism for aligning nodes in the tree that otherwise have no distinct identity. This is important when comparing configurations and tracking change history to avoid flagging "false positive" differences. It also aids in specifying search criteria and crafting SQL queries used in compliance rules.

There are four varieties of base parser:

- XML
- Format-specific
- Columnar
- Properties

Some parsers have out-of-box default rules. These rules address well-known instances where nodes need to be aligned. Specifically, the WebLogic and WebSphere parsers contain default rules to address such instances. You can leave these rules as is, execute a subset of them, or replace them with your own custom rules.

This section covers the following topics:

- [Managing Parsers](#)
- [About XML Parsers](#)
- [About Format-Specific Parsers](#)
- [About Columnar Parsers](#)
- [About Properties Parsers](#)
- [Using Parsed Files and Rules](#)

26.7.1 Managing Parsers

While creating, editing, or viewing custom configurations, you can peruse the list of available parsers, their default parameters, and post-parser rules, if applicable. Parser

parameters dictate formatting such as comment character, delimiters, start and end characters, and so forth. You cannot edit these parameters, but you can export a parser as an XML file, edit the file, and import it back into the application under a new name. Some parsers also have default rules that serve to align nodes in the parsed tree for purposes of comparison, for example.

1. While working with a custom configuration, click **Manage Parsers**. A list of available parsers appears in a table. The column on the right (Base Parsers) denotes a general parser category, Properties for example, which implies file types that contain name/value pairs.
2. Select a parser and click **Details**. This dialog also shows default rules, if any.
 - Click the **Parameters** tab to see the parameter defaults in effect. You can then judge if you need to edit the parser to conform with your file format conventions.
 - Click the **Default Rules** tab to see the post-parsing rules that ship with certain parsers. This is a good way to get exposure to rules formation.
3. Assume you want to change the delimiter character in a given parser.
 - a. With the parser selected in the table, click **Export**.
 - b. In the dialog that opens click **Save** and navigate to a file system location. Save the XML file with an appropriate name.
 - c. In making your edits, be sure to change the parser ID and parser name in the XML, as you are creating a customized version of an out-of-box parser.
4. Assume you now want to import the new parser you saved for use in creating custom configurations.
 - a. With the Parsers table open, click **Import**.
 - b. In the dialog that opens, browse to the file location where you saved the exported parser file. Select it and click **Import** on the dialog.

The new parser now appears in the Parsers table where it can be used in custom configuration creation.

26.7.2 About XML Parsers

Cloud Control has two XML parsers: a default (attribute-keyed) XML parser and a generic XML parser.

26.7.2.1 About the Default XML Parser

Parsing occurs as follows:

- XML elements with no XML attributes or child elements become parsed attributes; all other elements become containers.
- XML attributes become parsed attributes.
- Element text content becomes a parsed attribute, with its name dependent on whether or not the tag contains any XML attributes. If the tag contains XML attributes, the parsed attribute name takes the value specified in the `STORE_CONTENT_AS` parameter; otherwise, the parsed attribute name takes the tag name.

The default XML parser accepts the following parameters:

Parameter	Description
MULTIKEY_DELIMITER	Delimiter that separates a list of XML attribute names in the CONTAINER_NAME parameter; default is tilde (~)
STORE_CONTENT_AS	Name to give to parsed attributes derived from element text content, where the element contains XML attributes; default is text_value
CONTAINER_NAME	<p>A list of XML attribute names delimited by the value of the MULTIKEY_DELIMITER parameter. If an attribute name in this list appears in a tag in the original file, the tag becomes a container named for the value of the XML attribute. All other XML attributes become parsed attributes as usual. The tag name itself is discarded.</p> <p>For example, the list includes attribute names Moe and Larry in this order. The original file contains an XML tag Stooges that has attributes Moe, Larry, and Curly. As Moe appears first in the delimited list, its value, leader, becomes the parsed container name; Larry and Curly become parsed attributes. The tag name Stooges is discarded. The original XML fragment might be as follows:</p> <pre><?xml version="1.0" encoding="UTF-8"?> <Comedy> <Stooges Moe="leader", Larry="zany", Curly="bald"> </Stooges> </Comedy></pre>

WebLogic Attribute-keyed Parser

Cloud Control provides an out-of-box attribute-keyed parser specifically designed to parse the WebLogic `config.xml` file. It has the same parameters as the default XML parser and comes with 26 default post-parsing rules to uniquely identify nodes with the same name.

WebSphere Attribute-keyed Parsers

Cloud Control provides several out-of-box attribute-keyed parsers designed to parse specific WebSphere configuration files. Each parser has the same parameters as the default XML parser and comes with a set of default post-parsing rules to uniquely identify nodes with the same name. There are parsers for the following WebSphere configuration files:

- `node.xml` (1 default post-parsing rule)
- `plugin-cfg.xml` (7 default post-parsing rules)
- `resource.xml` (9 default post-parsing rules)
- `server.xml` (13 default post-parsing rules)
- `variables.xml` (1 default post-parsing rule)

26.7.2.2 About the Generic XML Parser

Parsing occurs as follows:

- All XML elements become containers.
- All XML attributes become parsed attributes.
- Element text content becomes a parsed attribute that takes the name `text_value`, where the text content becomes the parsed attribute value.

The generic XML parser accepts no parameters.

WebSphere Generic Parser

Cloud Control provides one out-of-box generic parser designed to parse the WebSphere `serverindex.xml` configuration file. It comes with three default post-parsing rules to uniquely identify nodes with the same name.

26.7.2.3 XML Parser Examples

This section contains three XML parser examples:

- As parsed using the default XML parser, with out-of-box parameter values
- As parsed using the default XML parser, with modified parameter values
- As parsed using the generic XML parser

Parsed examples derive from the following original XML file:

```
<?xml version="1.0" encoding="UTF-8"?>
<Application>
  <AppName>foo</AppName>
  <Server name="ajax" os="linux">production</Server>
</Application>
```

Default XML Parser (Out-of-Box Parameter Values)

When parsed using the default XML parser with out-of-box parameter values, the parsed version appears as follows:

```
Application
  AppName = foo
  Server
    name = ajax
    os = linux
    text_value = production
```

Note the following about this parsed version:

- The element contents of the `AppName` and `Server` tags become parsed attributes.
- Since the `AppName` tag contains no XML attributes, the parsed attribute name takes the tag name.
- Contrast with the `Server` tag, which has XML attributes (`name` and `os`). This results in a container named for the tag (`Server`), with three parsed attributes, one for each of the XML attributes, and a third for the text content of the `Server` tag, which is set to the value of the `STORE_CONTENT_AS` parameter (`text_value`).

Default XML Parser (Modified Parameter Values)

To modify parameter values, you have to create a new parser by exporting the default XML parser, modifying the exported XML file, and importing the modified parser, using a new name and parser ID.

Assume you followed this process, making the following modifications:

- Set the `STORE_CONTENT_AS` parameter to the value `myVal`
- Set the `CONTAINER_NAME` parameter to the value `name`

When parsed using the default XML parser with modified parameter values, the parsed version appears as follows:

```
Application
```

```

AppName = foo
ajax
  os = linux
  myVal = production

```

Note the following about this parsed version:

- The AppName tag remains the same; that is, it has no XML attributes so it becomes a parsed attribute.
- Since the Server tag has an XML attribute that matches the value of CONTAINER_NAME, the container takes the value of the attribute (ajax), obviating the name=ajax parsed attribute. Remember that the out-of-box CONTAINER_NAME parameter has a placeholder but no actual default value; thus, the difference in this version of the parsed representation.
- The remaining Server tag attribute (os) becomes a parsed attribute as usual, and the text content associated with the tag becomes the value of the attribute myVal, per the edited STORE_CONTENT_AS parameter.

Generic XML Parser

When parsed using the generic XML parser (the one that takes no parameters), the parsed version appears as follows:

```

Application
  AppName
    text_value = foo
  Server
    name = ajax
    os = linux
    text_value = production

```

Refer to [Section 26.7.2.1](#) for a reminder of how parsing occurs.

26.7.3 About Format-Specific Parsers

Format-specific base parsers are applicable only to a particular data format. Format-specific parsers run the gamut from having no parameters to a few to many with which to tailor formatting.

Parser	Description
Blue Martini DNA	Parser for Blue Martini DNA files (no parameters).
Connect:Direct	Parser for Connect:Direct .cfg files (no parameters).
Database Query (see Section 26.7.6.3 for an example)	Parser for custom configuration database query output. Cloud Control automatically transforms query results into a format the parser accepts, organizing results into sections similar to a Windows .ini file. Each section represents one record; each line in a section contains a table column name and a value. See Section 26.7.3.1 .
Db2	Parser for the output of the DB2 GET DATABASE CONFIGURATION command (no parameters).
Directory	Parser for files containing multiple name value pairs on the same line, where each line may have varying numbers of pairs. For example, the first line might be a=b j=k, the second line c=d m=n y=z, and so forth. See Section 26.7.3.2 .

Parser	Description
E-Business Suite	Parser for E-Business Suite <code>.drv</code> files. The parser converts <code>IF . . . THEN . . . ELSE</code> structures in the file into containers in the parsed representation, and the rest of the lines into a container with a fixed number of parsed attributes. These lines can be of two types: directory specifications, whose parsed attribute names are specified in the <code>DIR_HEADER</code> parser parameter; configuration file specifications, whose parsed attribute names are specified in the <code>HEADER</code> parser parameter. See Section 26.7.3.3 .
Galaxy CFG	Parser for Galaxy <code>.cfg</code> files. See Section 26.7.3.4 .
Introscope	Parser for Introscope files (no parameters).
MQ-Series	Parser for MQ-Series files. See Section 26.7.3.5 .
Odin	Parser for Odin files (no parameters).
Oracle ORA	Parser for Oracle <code>.ora</code> files, such as <code>tnsnames.ora</code> (no parameters).
Siebel	Parser for Siebel <code>siebns</code> files. The parser creates a container for each unique path in the file, and attributes for name value pairs, except where a line contains the string <code>Type=empty</code> , in which case the parser does not create a parsed attribute for the line. See Section 26.7.3.6 .
UbbConfig	Parser for BEA Tuxedo files (no parameters). The parser converts sections prefixed with an asterisk (*), and names in double quotes at the start of a new line, into containers. It converts all other data into attributes.
Unix Installed Patches	Parser for Unix installed patches data. The parser creates one container per (non-comment) line of the file. It treats every field ending with a colon (:) on each line as a property name field and the value following, if any, as the property value. Note that a property does not have to have a value. See Section 26.7.3.7 .
Unix Recursive Directory List	Parser for output of Unix recursive directory listing (<code>ls -l -R</code>). The parser converts each subdirectory line into a container, and each file information line into a container with a fixed set of attributes. See Section 26.7.3.8 .

Remember, to modify a format-specific parser, you have to create a new parser by exporting the particular parser, modifying the exported XML file, and importing the modified parser, using a new name and parser ID.

26.7.3.1 Database Query Parser Parameters

The following table describes the parameters with which you can customize the Database Query parser:

Parameter	Description
<code>CELL_DELIMITER</code>	Character that separates name value pairs; default is <code>=</code> .
<code>PROPERTY_DELIMITER</code>	Character that separates the length of a name or value from the value itself; default is <code>_</code> .
<code>COMMENT</code>	Character that tells the parser to ignore the line that follows; default is <code>#</code> .
<code>SECTION_START</code>	Character that denotes the start of a section; default is <code>\[</code> (backslash is escape character).
<code>SECTION_END</code>	Character that denotes the end of a section; default is <code>\]</code> (backslash is escape character).

Parameter	Description
USE_INI_SECTION	Flag that tells the parser to use Windows .ini type sections; default is true.

26.7.3.2 Directory Parser Parameters

The following table describes the parameters with which you can customize the Directory parser:

Parameter	Description
CELL_DELIMITER	Character that separates one property from another; default is a space.
EXTRA_DELIMITER	Character that separates a property name from its value; default is =.
COMMENT	Character that tells the parser to ignore the line that follows; default is #.

26.7.3.3 E-Business Suite Parser Parameters

The following table describes the parameters with which you can customize the E-Business Suite parser:

Parameter	Description
DIR_HEADER	A tilde-delimited list of attribute names for directory specifications.
STRUCTURE_START	A tilde-delimited list of regular expressions denoting the start of a structure.
CELL_DELIMITER	A tilde-delimited list of regular expressions denoting name value pair delimiters.
HEADER	A tilde-delimited list of attribute names for file specifications.
COMMENT	A tilde-delimited list of regular expressions denoting comments.
STRUCTURE_END	A tilde-delimited list of regular expressions denoting the end of a structure.
LAST_FREE_FORM	Flag that tells the parser to ignore cell delimiters in the last value of a directory or file specification; default is true.
ELEMENT_FIELD	A tilde-delimited list of file specification attribute names. The parser concatenates values of the specified attributes to form the name of the container associated with the file specification.
DIR_ELEMENT_FIELD	A tilde-delimited list of directory specification attribute names the parser uses to determine the name of the container associated with the directory specification.

26.7.3.4 Galaxy CFG Parser Parameters

The following table describes the parameters with which you can customize the Galaxy CFG parser:

Parameter	Description
COMMENT	Character that tells the parser to ignore the line that follows; default is !.
ADD_SUFFIX	Names of attributes whose values to append to a container name.

Parameter	Description
MONO_PROP_SECTION	Names of sections that have a single property.
MULTI_PROP_SECTION	Names of sections that have multiple properties.
NODES_SECTION	Names of section start and end elements

26.7.3.5 MQ-Series Parser Parameters

The MQ-Series parser has a single parameter that you can customize: `COMMENT`, which defaults to `*`.

26.7.3.6 Siebel Parser Parameters

The following table describes the parameters with which you can customize the Siebel parser:

Parameter	Description
LINES_TO_SKIP	Tells the parser the number of lines to ignore at the beginning of the file; default is 4.
CELL_DELIMITER	A tilde-delimited list of regular expressions denoting name value pair delimiters.
COMMENT	A tilde -delimited list of regular expressions denoting comments.
SECTION_START	A tilde-delimited list of regular expressions denoting the start of a unique path specification section.
SECTION_END	A tilde-delimited list of regular expressions denoting the end of a unique path specification section.
USE_INI_SECTION	Flag that tells the parser to use Windows <code>.ini</code> type sections; default is true.

26.7.3.7 Unix Installed Patches Parser Parameters

The following table describes the parameters with which you can customize the Unix Installed Patches parser:

Parameter	Description
CELL_DELIMITER	Character that separates name value pairs; default is a space.
EXTRA_DELIMITER	Character that separates a property name from its value; default is <code>∴</code> .
COMMENT	Character that tells the parser to ignore the line that follows; default is <code>#</code> .

26.7.3.8 Unix Recursive Directory List Parser Parameters

The following table describes the parameters with which you can customize the Unix Recursive Directory List parser:

Parameter	Description
LINES_TO_SKIP	Tells the parser the number of lines to ignore at the beginning of the file; default is 4.
CELL_DELIMITER	A tilde-delimited list of regular expressions denoting name value pair delimiters.

Parameter	Description
COMMENT	A tilde-delimited list of regular expressions denoting comments.
HEADER	A tilde-delimited list of attribute names.
LAST_FREE_FORM	Flag that tells the parser to ignore cell delimiters in the last value of a line; default is true.
SECTION_START	A tilde-delimited list of regular expressions denoting the start of a subdirectory section.
SECTION_END	A tilde-delimited list of regular expressions denoting the end of a subdirectory section.
ELEMENT_FIELD	A tilde-delimited list of attribute names. The parser concatenates values of the specified attributes to form the name of the container associated with the line.

26.7.4 About Columnar Parsers

Columnar parsers are inherently flexible owing to the parameters they can accept to tailor formatting. All columnar parsers use a subset of the same parameters.

Parser	Description
Cron Access	Parser for <code>cron.allow</code> and <code>cron.deny</code> files.
Cron Directory	Parser for <code>Unix etc</code> and <code>cron.d</code> files.
CSV	Parser for comma-separated-value data. The out-of-box parameter values support CSV files with these characteristics: <ul style="list-style-type: none"> ▪ Each line has the same number of values ▪ The first parsed (that is, non-comment) line is a header line whose content is a comma-separated list of column names ▪ Commas in double quotes are considered part of the value, not value delimiters ▪ One of the column names is "name" whose value becomes the container name associated with each line Text inside double quotes is considered part of a value; to specify a value that contains a double quote, escape the double quote with a backslash (\). Use a backslash to escape the backslash character itself (\\).
Hosts Access	Parser for <code>hosts.allow</code> and <code>hosts.deny</code> files.
Kernel Modules	Parser for <code>kernel modules</code> files.
Linux Directory List	Parser for Linux directory listing data format (for example, output of a <code>ls -l</code> command).
PAM Configuration	Parser for <code>pam.conf</code> files.
PAM Directory	Parser for <code>Unix etc/pam.d</code> files.
Process Local	Parser for <code>process.local</code> files.
Secure TTY	Parser for <code>Unix etc/securetty</code> files.
Solaris Installed Packages	Parser for Solaris installed packages files.
Unix Crontab	Parser for <code>Unix crontab</code> files.
Unix Directory List	Parser for Unix directory listing data format for example, the output of a <code>ls -l</code> command).

Parser	Description
Unix Groups	Parser for Unix <code>etc/group</code> files. The parser ignores group name and password information.
Unix GShadow	Parser for Unix <code>etc/gshadow</code> files.
Unix Hosts	Parser for Unix <code>etc/hosts</code> files.
Unix INETD	Parser for Unix <code>etc/inetd.conf</code> files.
Unix Passwd	Parser for Unix <code>etc/passwd</code> files. The parser ignores password values.
Unix Protocols	Parser for Unix <code>etc/hosts</code> files.
Unix Services	Parser for Unix <code>etc/services.conf</code> files.
Unix Shadow	Parser for Unix <code>etc/shadow</code> files.
Unix System Crontab	Parser for Unix system crontab files. System crontab files are very similar to crontab files, but may contain name value pairs such as <code>PATH=/a/b</code> .

26.7.4.1 Columnar Parser Parameters

This section describes all columnar base parser parameters. Although the base parser can accept values for any of these parameters, a given parser specification does not necessarily need to provide values for all of them. All parameters have default values, which are used in the absence of a specified value, although in some cases, parameters have explicit values.

Use quotes when delimiters or other special text such as comment characters or new lines are part of some value. The `QUOTE_DELIMITER` determines the character value to use. Prefix the quote delimiter with a backslash (`\`) if you need to escape the character. Use a backslash to escape the backslash character itself (`\\`) in quoted strings.

Parameter	Description
<code>COMMENT</code>	A tilde-delimited list of regular expressions that denote comment characters or sequences. For example, <code>#[^\r\n]*</code> specifies that everything on a line following the <code>#</code> character is a comment. Default is an empty list; that is, parse all file contents.
<code>LINES_TO_SKIP</code>	The number of initial lines (excluding blank or comment lines) to ignore for parsing purposes, treating them in effect as comments. Default is 0; that is, skip no lines.
<code>CELL_DELIMITER</code>	A tilde-delimited list of regular expressions that delimit line values. Default is an empty list; that is, no delimiters (it is unusual to use the default).
<code>QUOTE_DELIMITER</code>	A tilde-delimited list of regular expressions that define how quoted values begin and end (usually either a single or double quote character). The beginning and end quote delimiter must be the same. Default is an empty list; that is, parser does not recognize quoted values.
<code>PROPERTY_DELIMITER</code>	A tilde-delimited list of regular expressions that delimit property names and values. Default is an empty list; that is, no property delimiters. Rarely, a columnar file may contain name value pairs of the syntax <code>a=b</code> .

Parameter	Description
RESERVED_DIRECTIVES	A tilde-delimited list of property keywords. Some crontab files contain lines of simple name value pairs, separated by a delimiter (foo=bar), thus violating the requirement that each line have the same number of fields. This parameter provides a workaround to specify property keywords. In the example, the property keyword would be foo. This says, in effect, parse any line beginning with this keyword as a parsed attribute name value pair under the root container. Default is an empty list; that is, no property keywords.
ALTERNATE_DELIMITER	An alternate delimiter for property names and values. Default is '/' (used only if ALTERNATE_FIELD parameter is nonempty).
ALTERNATE_FIELD	A tilde-delimited list of fields separated by alternate delimiters. Default is an empty list; that is, no alternate delimiters.
HEADER_FLAG	A flag specifying whether or not the file has a header line that specifies the column names. Default is false.
HEADER	A tilde-delimited list of column names to use if there is no header line. Default is an empty list; that is, no column names (it is unusual to use the default).
ELEMENT_FIELD	A tilde-delimited list of column names whose values the parser concatenates to create the container name associated with a line. Default is an empty list; that is, no column names (it is unusual to use the default).
IGNORE_FIELD	A tilde-delimited list of column names to ignore. No parsing of values in these columns occurs. Default is an empty list; that is, ignore nothing.
LAST_FREE_FORM	A flag that specifies whether the last column is free form. The parser ignores all delimiters in a free form column value. Default is false.
USE_LINE_COMMENT	A flag that specifies whether to treat end of line comments as a value to appear in the parsed representation of the data. Default is false.

26.7.5 About Properties Parsers

Properties parsers are inherently flexible owing to the parameters they can accept to tailor formatting and handle disparate organizational elements. All properties parsers use the same set of basic and advanced parameters, as well as advanced constructs.

Parser	Description
AIX Installed Packages	Parser for AIX installed packages files.
Apache HTTPD	Parser for Apache HTTPD.conf files.
Autosys	Parser for Autosys.jil files.
Custom CFG	Parser for custom .cfg files. This syntax defines an element with E = {} syntax, where the brackets may contain name value pairs, nested elements, or both.
Java Policy	Parser for java.policy files.
Java Properties	Parser for java.properties files.
LDAP	Parser for LDAP .cfg files.
Mime Types	Parser for mime.types files.
Radia	Parser for Radia .cfg files.

Parser	Description
Sectioned Properties	Parser for files containing name value pairs organized into sections, such as a Windows .ini file.
SiteMinder Agent	Parser for SiteMinder agent files.
SiteMinder Registry	Parser for SiteMinder .registry files.
SiteMinder Report	Parser for SiteMinder SmReport.txt files.
SmWalker	Parser for SiteMinder SmWalker.dat files.
Sun ONE Magnus	Parser for Sun ONE magnus.conf files.
Sun ONE Obj	Parser for Sun ONE obj.conf files.
Tuxedo	Parser for Tuxedo files.
Unix Config	Parser for Unix etc/config files.
Unix Login	Parser for Unix etc/login.defs files.
Unix PROFTPD	Parser for Unix etc/proftpd.conf files.
Unix Resolve	Parser for Unix etc/resolve.conf files.
Unix SSH Config	Parser for Unix etc/ssh/sshd.conf files.
Unix System	Parser for Unix etc/system files.
Unix VSFTPD	Parser for Unix etc/vsftpd.conf files.
Unix XINETD	Parser for Unix etc/xinetd.conf files.
WebAgent	Parser for WebAgent files.
Windows Checksum	Parser for Windows checksum output generated with fciv.exe.

26.7.5.1 Basic Properties Parser Parameters

This section describes basic properties parser parameters that are required to parse simple property data formats. Simple property data formats specify a property as a name value pair, usually with a defined delimiter separating the name and the value: foo=bar. The basic data format is a list of properties, one property to a line, together with optional comments; a java.properties file, for example. All parameters have default values, which are used in the absence of a specified value.

Use quotes when delimiters or other special text such as comment characters or new lines are part of some value. The QUOTE_DELIMITER determines the character value to use. Prefix the quote delimiter with a backslash (\) if you need to escape the character. Use a backslash to escape the backslash character itself (\) in quoted strings.

A comment character such as the pound sign (#), or a particular character sequence (//) usually denotes a comment. Special sequences such as a C style comment (/...*/) might denote the beginning and end of a comment. Some files might have generic informational content in the first couple of lines. In this case, a parameter is available to tell the parser to ignore these lines.

Parameter	Description
COMMENT	A tilde-delimited list of regular expressions that denote comment characters or sequences. For example, #[^\r\n]* specifies that everything on a line following the # character is a comment. Default is an empty list; that is, parse all file contents.

Parameter	Description
LINES_TO_SKIP	The number of initial lines (excluding blank or comment lines) to ignore for parsing purposes, treating them in effect as comments. Default is 0; that is, skip no lines.
CELL_DELIMITER	A tilde-delimited list of regular expressions that delimit line values. Default is an empty list; that is, no delimiters (it is unusual to use the default).
QUOTE_DELIMITER	A tilde-delimited list of regular expressions that define how quoted values begin and end (usually either a single or double quote character). The beginning and end quote delimiter must be the same. Default is an empty list; that is, parser does not recognize quoted values.
ALLOW_NAME_ONLY_PROPERTIES	A flag that indicates whether the parser allows property names without a delimiter or a value. Default: false.
REVERSE_PROPERTY	A flag that indicates whether the parser allows the value to come before the delimiter and property name. Default: false.

26.7.5.2 Advanced Properties Parser Parameters

This section describes advanced properties parser parameters that are required to parse more complex property data formats. All parameters have default values, which are used in the absence of a specified value.

Parameter	Description
PROPERTY_DELIMITER	A tilde-delimited list of regular expressions denoting property delimiters. For example, the text "a=b : x=y" could be interpreted in either of two ways: <ul style="list-style-type: none"> ■ As a single property "a" with value "b : x=y" ■ As two separate properties, "a=b" and "x=y" If a colon (:) is the property delimiter, the parsing engine interprets the text as containing two separate properties. Default is an empty list; that is, parser does not recognize property delimiters.
LINE_END_DELIMITER	A tilde-delimited list of regular expressions denoting line end sequences. When the parser encounters a line end delimiter, it assumes a new property or construct starts on the next line. Default is an empty list; that is, parser does not recognize line end delimiters.
CONTINUE_LINE	A tilde-delimited list of regular expressions denoting continue line sequences. When the parser encounters a continue line pattern, it interprets data on the following line as a continuation of the construct or property on the previous line, as opposed to interpreting the new line as the beginning of a new property or construct. For example, the parser must encounter a line continuation pattern to recognize property values that span multiple lines. Default is an empty list; that is, parser does not recognize line continuation patterns.
SECTION_START	A tilde-delimited list of regular expressions denoting the beginning of a section. Sections cannot be nested. Default is an empty list; that is, parser does not recognize sections.
SECTION_END	A tilde-delimited list of regular expressions denoting the end of a section. Default is an empty list.
STRUCTURE_START	A tilde-delimited list of regular expressions denoting the beginning of a structure. Structures can be nested. Default is an empty list; that is, parser does not recognize structures.

Parameter	Description
STRUCTURE_END	A tilde-delimited list of regular expressions denoting the end of a structure. Default is an empty list.
XML_STYLE_TAG	A flag that indicates whether structures in the file are XML style tags. Default: false.
USE_INI_SECTION	A flag that indicates whether INI style sections are present. Default: false.
RESERVED_DIRECTIVES	A tilde-delimited list of reserved names indicating the start of a reserved directive. Default is an empty list; that is, parser does not recognize reserved directives.
RESERVED_FUNCTIONS	A tilde-delimited list of reserved names indicating the start of a reserved function. Default is an empty list; that is, parser does not recognize reserved functions.
DIRECTIVE_PROPERTIES	A tilde-delimited list of reserved directive- implicit property names. Default is an empty list.
FUNCTION_PROPERTIES	A tilde-delimited list of required reserved function-explicit property names. Default is an empty list.
SECTION_PROPERTIES	A tilde-delimited list of section-implicit property names. Default is an empty list.
STRUCTURE_PROPERTIES	A tilde-delimited list of structure-implicit property names. Default is an empty list.
ELEMENT_FIELD	A keyword to be ignored by the parser when parsing properties. This typically applies to data formats that specify a keyword before a name value pair; "set a=b" for example. Default is an empty list; that is, parser ignores nothing.
ALLOW_ELEMENT_CELL	A flag that indicates whether the file format supports element cell structures. Default: false.
SECTION_EXPLICIT_PROPERTIES	A flag that indicates whether sections support explicit properties. Default: false.
STRUCTURE_EXPLICIT_PROPERTIES	A flag that indicates whether structures support explicit properties. Default: false.
NEWLINE_CONTINUE_LIN	A flag that indicates whether newlines can be line continuation sequences. Default: false.
KEYWORD_FIELD	A tilde-delimited list of regular expressions denoting keywords that precede properties that use a whitespace delimiter. Default is an empty list; that is, parser does not recognize keywords.

26.7.5.3 Advanced Properties Parser Constructs

Properties files come in variety of file formats. To accommodate the widest possible range of formats, the generic properties base parser uses combinations of constructs found in most files.

The constructs fall into two categories:

- Container constructs, which can be reserved functions, reserved directives, XML structures, structures, delimited structures, INI sections, delimited sections, sections, and element cells
- Property constructs, which can be simple properties, reverse properties, keyword properties, keyword name properties, bracket properties, implicit properties and explicit properties

Of the element constructs, section constructs cannot be nested, but can contain any other construct. Structure constructs can be nested, and can contain any construct except a section. Element cells can be nested, but can only contain element cells and simple properties. Reserved directives and reserved functions cannot be nested, nor can they contain any other constructs.

The rest of this section describes the constructs the base properties parser supports.

Simple Property

A simple property consists of a property name, cell delimiter, property value, and newline sequence, in that order. A simple property may take up more than one line, although properties that span multiple lines usually contain a line continuation character or sequence. The parser ignores whitespace such as tabs and spaces, unless a parameter specifies whitespace as having some significance (cell delimiter, for example).

Example: `name=value_that_wraps_to_next_line_/,` where the forward slash serves as a line continuation character. A Java Properties file typifies this data format.

Keyword Property

This construct is the same as a simple property, only with a keyword in front, which the parser ignores.

Example: `set name=value,` where `set` is the ignored keyword. A Unix System file typifies this data format.

Keyword Name Property

This construct is a simple property where the property name matches a regular expression specified in the `KEYWORD_FIELD` parser parameter. This is a special case property type specific to the Unix XINETD parser. The XINETD file uses an equal sign (=) as a cell delimiter except when the property begins with the keyword "include" or "includedir", in which case the cell delimiter is whitespace.

While added specifically for XINETD files, the property can be used for other file types where appropriate.

Example: `includedir /etc,` where `includedir` is the parser parameter regular expression and whitespace is the cell delimiter.

Explicit Property

An explicit property consists of a property name, a delimiter, and a property value. Unlike a simple or keyword property, an explicit property is bound to a container construct such as a section or a structure; an XML tag attribute, for example.

Examples:

```
[SectionName p1=v1 p2=v2]
<StructureName p1=v1 p2=v2>
...
</StructureName>
```

In these constructs, the name value pairs `p1 v1` and `p2 v2` are explicit properties. A Sun ONE Obj file typifies this data format.

Implicit Property

An implicit property is a property value without an associated property name. Like an explicit property, an implicit property is bound to a container construct, usually a

reserved directive. The `DIRECTIVE_PROPERTIES` parser parameter contains the property names of implicit properties.

Examples:

```
[SectionName myName myPath]

<StructureName myName myPath>
...
</StructureName>
```

In these constructs, the implicit properties have the values `myName` and `myPath`, with the presumed property names `name` and `path`, as declared in the `DIRECTIVE_PROPERTIES` parser parameter. An Apache HTTPD file typifies this data format.

Reserved Function

A reserved function is a keyword followed by one or more explicit properties. The `RESERVED_FUNCTIONS` parser parameter specifies keywords that denote reserved functions.

Example: `Error fn="query-handler" type="forbidden"`, where `Error` is the reserved function keyword specified in the `RESERVED_FUNCTIONS` parser parameter. A Sun ONE Magnus file typifies this data format.

Reserved Directive

A reserved directive is a keyword followed by one or more implicit properties. The `RESERVED_DIRECTIVES` parser parameter specifies keywords that denote reserved directives.

Example: `LoadModule cgi_module "/bin/modules/std/cgi"`, where `LoadModule` is the reserved function keyword specified in the `RESERVED_DIRECTIVES` parser parameter. An Apache HTTPD file typifies this data format.

XML Structure

An XML structure is a standard XML tag that can contain a name only, a name followed by explicit properties, or a name followed by implicit properties.

Examples:

```
<Name>
...
</Name>

<Name p1=v1 p2=v2>
...
</Name>
<Name "implicit_property1" "implicit_property2">
...
</Name>
```

A WebAgent file typifies this data format.

Delimited Structure

A delimited structure consists of the following (in the specified order):

- Structure name
- Delimiter
- Start structure character or character sequence

- Structure contents
- End structure character or character sequence

Example:

```
StructureName = {  
  ...  
}
```

Explicit and implicit properties are not allowed. Java Policy and Custom CFG files typify this data format.

Structure

A structure consists of the following (in the specified order):

- Structure name
- Start structure character or character sequence
- Structure contents
- End structure character or character sequence

The only difference between a delimited structure and a structure is the delimiter; that is, a structure does not require a delimiter between the structure name and the start structure indicator.

Example:

```
StructureName {  
  ...  
}
```

Explicit and implicit properties are not allowed. A Unix XINETD file typifies this data format.

INI Section

And INI section resembles a section heading in a Windows `.ini` file, characterized by:

- Section start character or character sequence
- Section name
- Optional (explicit and implicit) properties
- Section end character or character sequence

Examples:

```
[SectionName]
```

```
[SectionName p1=v1 p2=v2]
```

```
[SectionName "implicit_property1" "implicit_ property2"]
```

SmWalker and Sectioned Properties files typify this data format.

Delimited Section

A delimited section is a line that begins with a common pattern, but otherwise resembles a simple property.

Examples:

```
HKEY_LOCAL_MACHINE\SOFTWARE\A\B\C=789
```

```
HKEY_LOCAL_MACHINE\SOFTWARE\X\Y\Z=123
```

These are two delimited section headings where the common pattern is `HKEY_`. SiteMinder Registry and LDAP files typify this data format.

Element Cell

An element cell consists of an element cell name and a property name value pair of the form `A = B = C`. Element cells typically use line continuation sequences and nesting to clarify the structure. An element cell that has multiple properties uses a property delimiter to separate them.

Example 1:

```
EC = \
    B = C, D = F
```

This example is an element cell named `EC` with two property name value pairs, `B = C` and `D = F`, separated by a comma. The structure uses the backslash character (`\`) to indicate line continuation. The advanced properties parser parameters `PROPERTY_DELIMITER` and `CONTINUE_LINE` define the respective format characters.

Example 2:

```
EC = \
    EC2 = \
        A = B, \
        C = D
```

This example is an element cell named `EC` that has a nested element cell named `EC2` that contains two property name value pairs, `A = B` and `C = D`. This example uses the same delimiter and line continuation characters.

26.7.6 Using Parsed Files and Rules

A collected configuration file is stored in raw form and, if a parser is specified, in a tree structure of nodes, or containers, and attributes, or properties. The file also is generated internally in XML format for the purpose of applying post-parsing rules, which consist of XPath conditions and expressions. Note that even non-XML files are generated in this internal format. Since the internal format must accommodate other file types, it introduces an additional root node in the XML to compensate for files such as Java properties files that have only attribute names and values.

Examples of how files are parsed and displayed, and the effects of post-parsing rules help to clarify:

- [Sample XML File Parsing and Rule Application](#)
- [Sample Non-XML File Parsing and Rule Application](#)
- [Sample SQL Query Parsing and Rule Application](#)

26.7.6.1 Sample XML File Parsing and Rule Application

Consider the following simple XML file:

```
<dir name="/a/b/c">
  <file name="file1" size=120/>
```

```

    <file name="file2" size=350/>
  </dir>

```

Its parsed form, using the default XML parser, appears in the user interface in the following tree structure:

```

dir
  name = /a/b/c
  file
    name = file1
    size = 120
  file
    name = file2
    size = 350

```

Notice that two containers have the same name (file), which makes it impossible to distinguish between the two, at the container level, at least. Thus, this file is a candidate for a post-parsing rule. As mentioned, there is a special internal XML format against which to apply a rule's XPath condition and expression. This format treats nodes and attributes as XML elements, and converts attribute values into corresponding element text content. It also adds a root element that doesn't appear in the original file:

```

<root>

  <dir>
    <name>/a/b/c</name>
    <file>
      <name>file1</name>
      <size>120</size>
    </file>
    <file>
      <name>file2</name>
      <size>350</size>
    </file>
  </dir>
</root>

```

Given the problem in the parsed form of having two containers with the same name, a rule resolution might consist of the following:

Condition: `/root/dir/file`

Expression: `name/text()`

Effectively, this says: for each file evaluate `name/text()` to produce an identifier that distinguishes one file from another within the `dir` node.

After applying the post-parsing rule, the parsed tree structure appears as follows:

```

dir
  name = /a/b/c
  file[file1]
    name = file1
    size = 120
  file[file2]
    name = file2
    size = 350

```

The rule resolves to an identifier appended in square brackets to the container name. The combination (`file[file1]`, for example) enables various operations such as compare, search, change history, and so forth, to distinguish between file containers.

26.7.6.2 Sample Non-XML File Parsing and Rule Application

Consider the following simple ORA file:

```
acme=
  (DESCRIPTION=
    (SOURCE_ROUTE=yes)
    (ADDRESS=(PROTOCOL=tcp)(HOST=host1)(PORT=1630))
    (ADDRESS_LIST=
      (FAILOVER=on)
      (LOAD_BALANCE=off)
      (ADDRESS=(PROTOCOL=tcp)(HOST=host2a)(PORT=1630))
      (ADDRESS=(PROTOCOL=tcp)(HOST=host2b)(PORT=1630)))
    (ADDRESS=(PROTOCOL=tcp)(HOST=host3)(PORT=1630))
    (CONNECT_DATA=(SERVICE_NAME=Sales.us.acme.com)))
```

Its parsed form, using the Oracle ORA parser, appears in the user interface in the following tree structure:

```
acme
  DESCRIPTION
    SOURCE_ROUTE    yes
    ADDRESS
      PROTOCOL      tcp
      HOST           host1
      PORT           1630
    ADDRESS_LIST
      FAILOVER      on
      LOAD_BALANCE  off
      ADDRESS
        PROTOCOL    tcp
        HOST         host2a
        PORT         1630
      ADDRESS
        PROTOCOL    tcp
        HOST         host2b
        PORT         1630
    ADDRESS
      PROTOCOL      tcp
      HOST           host3
      PORT           1630
    CONNECT_DATA
      SERVICE_NAME  Sales.us.acme.com
```

Notice that the address containers, both standalone and within ADDRESS_LIST are indistinguishable. Thus, this file is a candidate for a post-parsing rule. As mentioned, there is a special internal XML format against which to apply a rule's XPath condition and expression. This format treats nodes and attributes as XML elements, and converts attribute values into corresponding element text content. It also adds a root element that doesn't appear in the original file:

```
<root>
  <acme>
    <DESCRIPTION>
      <SOURCE_ROUTE>yes</SOURCE_ROUTE>
      <ADDRESS>
        <PROTOCOL>tcp</PROTOCOL>
        <HOST>host1</HOST>
        <PORT>1630</PORT>
      </ADDRESS>
    <ADDRESS_LIST>
```

```

        <FAILOVER>on</FAILOVER>
        <LOAD_BALANCE>off</LOAD_BALANCE>
        <ADDRESS>
            <PROTOCOL>tcp</PROTOCOL>
            <HOST>host2a</HOST>
            <PORT>1630</PORT>
        </ADDRESS>
        <ADDRESS>
            <PROTOCOL>tcp</PROTOCOL>
            <HOST>host2b</HOST>
            <PORT>1630</PORT>
        </ADDRESS>
    </ADDRESS_LIST>
    <ADDRESS>
        <PROTOCOL>tcp</PROTOCOL>
        <HOST>host3</HOST>
        <PORT>1630</PORT>
    </ADDRESS>
    <CONNECT_DATA>
        <SERVICE_NAME>Sales.us.acme.com</SERVICE_NAME>
    </CONNECT_DATA>
</DESCRIPTION>
</acme>
</root>

```

Given the problem in the parsed form of having containers with the same name, a rule resolution might consist of the following:

Condition: //ADDRESS
 Expression: /HOST/text()

Effectively, this says: for each address element evaluate /HOST/text() to extract the host name as the address identifier.

After applying the post-parsing rule, the parsed tree structure appears as follows:

```

acme
  DESCRIPTION
    SOURCE_ROUTE    yes
    ADDRESS[host1]
      PROTOCOL      tcp
      HOST           host1
      PORT           1630
    ADDRESS_LIST
      FAILOVER      on
      LOAD_BALANCE  off
      ADDRESS[host2a]
        PROTOCOL    tcp
        HOST         host2a
        PORT         1630
      ADDRESS[host2b]
        PROTOCOL    tcp
        HOST         host2b
        PORT         1630
    ADDRESS[host3]
      PROTOCOL      tcp
      HOST           host3
      PORT           1630
    CONNECT_DATA
      SERVICE_NAME  Sales.us.acme.com

```


The rule resolves to an identifier appended in square brackets to the container name. The combination (ADDRESS [host2a]), for example) enables various operations such as compare, search, change history, and so forth, to distinguish between address containers.

26.7.6.3 Sample SQL Query Parsing and Rule Application

Consider the following three-column database table SERVER_DETAILS:

SERVER_NAME	ENVIRONMENT	HOSTED_APPLICATIONS
webserver-100	QA	5
webserver-200	PERFORMANCE	6
webserver-500	PRODUCTION	3

The SQL query expressed as part of the custom configuration creation is as follows:

```
select * from SERVER_DETAILS
```

This query returns the following raw output:

```
[row]
11_SERVER_NAME=13_ webserver-100
11_ENVIRONMENT=2_ QA
19_HOSTED_APPLICATIONS=1_5
[row]
11_SERVER_NAME=13_ webserver-200
11_ENVIRONMENT=11_ PERFORMANCE
19_HOSTED_APPLICATIONS=1_6
[row]
11_SERVER_NAME=13_ webserver-500
11_ENVIRONMENT=10_ PRODUCTION
19_HOSTED_APPLICATIONS=1_3
```

The Configuration Browser Source tab renders the data the same way.

Its parsed form, using the Database Query parser, appears in the user interface in the following tree structure:

```
row
  SERVER_NAME=webserver-100
  ENVIRONMENT=QA
  HOSTED_APPLICATIONS=5
row
  SERVER_NAME=webserver-200
  ENVIRONMENT=PERFORMANCE
  HOSTED_APPLICATIONS=6
row
  SERVER_NAME=webserver-500
  ENVIRONMENT=PRODUCTION
  HOSTED_APPLICATIONS=3
```

Notice that the row containers are indistinguishable. Thus, this query result is a candidate for a post-parsing rule. As mentioned, there is a special internal XML format against which to apply a rule's XPath condition and expression. This format treats nodes and attributes as XML elements, and converts attribute values into corresponding element text content. It also adds a root element that doesn't appear in the original file:

```
<root>
```

```

<row>
    <SERVER_NAME>webserver-100</SERVER_NAME>
    <ENVIRONMENT>QA</ENVIRONMENT>
    <HOSTED_APPLICATIONS>5</HOSTED_APPLICATIONS>
</row>
<row>
    <SERVER_NAME>webserver-200</SERVER_NAME>
    <ENVIRONMENT>PERFORMANCE</ENVIRONMENT>
    <HOSTED_APPLICATIONS>6</HOSTED_APPLICATIONS>
</row>
<row>
    <SERVER_NAME>webserver-500</SERVER_NAME>
    <ENVIRONMENT>PRODUCTION</ENVIRONMENT>
    <HOSTED_APPLICATIONS>3</HOSTED_APPLICATIONS>
</row>
</root>

```

Given the problem in the parsed form of having three containers with the same name, a rule resolution might consist of the following:

Condition: /root/row/SERVER_NAME

Expression: SERVER_NAME/text ()

Effectively, this says: for each row evaluate SERVER_NAME/text () to produce an identifier that distinguishes one row from another within the tree structure.

After applying the post-parsing rule, the parsed tree structure appears as follows:

```

row[webserver-100]
    SERVER_NAME=webserver-100
    ENVIRONMENT=QA
    HOSTED_APPLICATIONS=5
row[webserver-200]
    SERVER_NAME=webserver-200
    ENVIRONMENT=PERFORMANCE
    HOSTED_APPLICATIONS=6
row[webserver-500]
    SERVER_NAME=webserver-500
    ENVIRONMENT=PRODUCTION
    HOSTED_APPLICATIONS=3

```

The rule resolves to an identifier appended in square brackets to the container name. The combination (row[webserver-100], for example) enables various operations such as compare, search, change history, and so forth, to distinguish between row containers.

26.8 Overview of Client Configurations

A "client" represents an end-user or customer system—a system that is not part of your own IT infrastructure. A "client configuration" represents the configuration data collected about the end-user's system. These configurations differ from the internal deployments that you manage using Cloud Control.

The Client System Analyzer (CSA) application allows Web server administrators to collect and analyze data from end-user systems. The client data is collected by an applet, diagnosed, and sent back to the CSA application. You can either use the CSA application that comes pre-installed with Cloud Control, or you can deploy CSA independently to your Web server.

To access client configurations, from the **Enterprise** menu, select **Configuration**, then select **Client Configurations**. See the Cloud Control online help for information on performing tasks related to client configurations.

This section covers the following topics:

- [About Client System Analyzer in Cloud Control](#)
- [Deploying Client System Analyzer Independently](#)

26.8.1 About Client System Analyzer in Cloud Control

Using the pre-installed application allows you to collect client data without having to set up a separate Web server. The Management Agents collect, analyze, and upload the client data to the Management Repository. End users do not need login credentials to access Cloud Control. Example usage scenarios include:

- End users who call the Help Desk may be asked to navigate to the out-of-box CSA page so that their system information is uploaded. The Technical Support Representative can then review the system information and offer solutions.
- The client's application can be changed to provide an "Upload my system information" link to the Client System Analyzer in the Cloud Control application. The link can specify certain configuration parameters, such as the URL to return to after the Client System Analyzer runs.
- The client's application can be modified to redirect its users to the Client System Analyzer in the Cloud Control page during login or at other points in the application. Collected information can then be used from within Cloud Control to obtain various bits of information about the client systems. Examples include most popular browser versions, or systems that do not have a necessary Operating System patch applied or do not have enough RAM.

To access the CSA application, from the **Enterprise** menu, select **Configuration**, then select **Client System Analyzer**. See the Cloud Control online help for information on working with the CSA application.

26.8.2 Deploying Client System Analyzer Independently

CSA can be deployed independently to any J2EE-capable Web server. This deployment strategy is appropriate when:

- Clients accessing CSA cannot reach or have limited access to a Cloud Control deployment; for example, due to a firewall.
- Further customization to the CSA application is required, such as:
 - Custom rules can be supplied to the CSA application so that the end users have immediate feedback as to whether their systems satisfy certain constraints.
 - The behavior of the applet can be changed to collect additional information or to present end users with additional or different user interfaces.
 - The load on the Management Service Web servers needs to be reduced.

Both pre-installed and standalone types of deployments assign a configurable identifier called a Client Configuration Collection Tag to every client configuration collection. After the client configuration data has been collected by the client configuration collection applet and written to the Web server directory specified by the CSA application, you must configure Cloud Control to collect the client configuration data and upload it to the Management Repository.

See the Cloud Control online help for information on collecting and viewing client configurations.

26.9 Overview of Relationships

Relationships define the associations that exist among targets, or more extensively, among managed entities. In general, relationships are inherent to a target type definition. But not all relationships can be anticipated at target type creation. Thus, Cloud Control supports creation of supplemental relationships. There are two methods available to create new relationships:

- Manually, by adding a generic system target
- Interactively, within the Configuration Topology Viewer

This section describes the manual process. For information on creating relationships within the Configuration Topology Viewer, see [Section 26.10.14](#).

There are two ways to access the generic system wizard:

- From the **Setup** menu, select **Add Target**, then select **Generic System**
- From the **Targets** menu, select **Systems**, then click the **Add** button

General

Provide general details of the generic system:

- Specify a meaningful target name
- Indicate whether this is to be a privilege-propagating system
- Set system properties such as cost center and life cycle status
- Add system members; there should be a logical correspondence to the selections
- Review member dependencies and indicate whether to include them
- Set the time zone appropriately (defaults to Greenwich Mean Time)

When done, click **Next**.

Define Associations

Select the check box to display any associations (relationships) that Cloud Control automatically detects based on the members added to the system. Add additional associations as follows:

1. Click **Add**.
2. Complete the dialog that opens as follows:
 - a. Select a member target in the left table. This populates the right table.
 - b. Select an associated target in the right table. This populates the association drop-down list.
 - c. Select the association you want to create.
 - d. Click **OK**. The new association appears in the associations table.
3. Click **Add** and repeat to create additional associations.

When done, click **Next**.

Availability Criteria

Use this page to declare the key members of the system; that is, the members that must be running for the system to be considered available. You can select any one, some, or all members, but you must select at least one.

When done, click **Next**.

Charts

Customize how you want charts to appear on the System Charts page:

- Supplement suggested charts with charts you add
- Edit certain suggested charts to fit your needs
- Deselect the suggested charts check box and customize the page entirely
- Alter the appearance of the Members page by adding and removing columns and abbreviations

When done, click **Next**.

Review

Verify the makeup of the generic system target. If everything appears in order, click **Finish**.

Upon confirmation that the target was successfully created, use the Configuration Topology Viewer to review and traverse the relationships you created.

26.10 Overview of Configuration Topology Viewer

The Configuration Topology Viewer provides a visual layout of a target's relationships with other targets.

This section covers the following topics:

- [About Configuration Topology Viewer](#)
- [Examples of Using Topology](#)
- [Viewing a Configuration Topology](#)
- [Determining System Component Structure](#)
- [Determining General Status of Target's Configuration Health](#)
- [Getting Configuration Health/Compliance Score of a Target](#)
- [Analyzing a Problem and Viewing a Specific Issue in Detail](#)
- [About Dependency Analysis](#)
- [About Impact Analysis](#)
- [Creating a Custom Topology View](#)
- [Deleting a Custom Topology View](#)
- [Excluding Relationships from a Custom Topology View](#)
- [Including Relationships to a Target in a Custom Topology View](#)
- [Creating a Relationship to a Target](#)
- [Deleting a Relationship from a Target](#)
- [Controlling the Appearance of Information on a Configuration Topology Graph](#)

26.10.1 About Configuration Topology Viewer

The Configuration Topology Viewer provides a visual layout of a target's relationships with other targets. To access the Configuration Topology Viewer from a target's home page, select **Configuration**, then select **Topology** in the dynamic target menu. A topology graph appears for the current target. Using the viewer, you can:

- Determine the source of a target's health problems, that is, detect which targets might be causing the failure. For example, a database is down because its host is down.
- Analyze the impact of a target on other targets. For example, the payroll and finance applications will be impacted if the database goes down.
- Determine the system's structure by viewing the members of a system and their interrelationships.
- Add additional relationships between targets. These relationships will be reflected in other Cloud Control tools.
- Customize your configuration topology views to focus on the targets for which you have responsibility.
- Share custom topology views that you have created with other Cloud Control users.

26.10.2 Examples of Using Topology

The following are examples of when to use the topology feature:

- Determine a system's component structure (see [Section 26.10.4](#))
- Analyze dependencies in relationships (see [Section 26.10.8](#))
- Analyze the impact of relationships (see [Section 26.10.9](#))

26.10.3 Viewing a Configuration Topology

The Configuration Topology Viewer provides a visual layout of a target's relationships with other targets.

In the situations where the topology you are viewing is larger than your browser window, you can adjust the view by:

- Clicking the small arrow icon in the bottom right corner of the window to bring up a navigator, which allows you to select which portion of the topology is in view.
- Decreasing the size of the nodes in the display using the zoom control in the top left of the display.

Perform the following steps:

1. Access the Configuration Topology Viewer.

From the **Targets** menu on the Cloud Control home page, select **All Targets**. In the table, click the appropriate target. On the resulting page, select **Configuration** then select **Topology** from the dynamic target menu.

2. From the **View** list, select any of the following:

- Uses

This view helps you determine the targets that the selected target depends on. If a target is having problems, this view can be useful in helping you

determine whether its problems have been caused by another target it depends on.

- Used By

This view shows you the targets that depend on the selected target. This can be useful, for example, if you are planning on shutting down the target and need to know what other targets will be affected

- System Members

This view shows the members of the system (available only for targets that are systems).

- Custom views that have been defined and shared by end users (custom views must be explicitly shared before they are available to others).

The Uses, Used By, and System Members views are out-of-box topology views. They cannot be modified.

3. The following operations are available on the Topology page:

- Create a custom topology view (see [Section 26.10.10](#))
- Delete a custom topology view (see [Section 26.10.11](#))
- Exclude relationships from a custom topology view (see [Section 26.10.12](#))
- Include relationships to a target in a custom topology view (see [Section 26.10.13](#))

26.10.4 Determining System Component Structure

To determine which components (targets and target components) comprise your IT system and their interrelationships, use the Configuration Topology Viewer.

Perform the following steps:

1. Access the Configuration Topology Viewer.
2. In the View menu, select **System Members** (available only if the target is a system). The view displays the relationships between the targets. The target type controls the default view that is shown.

To see the specific relationship between two targets, you can either hover over the link between them and the relationship name will pop up, or select **Link Labels** from the **Annotations** menu to display the relationship name on all links.

Note the following:

- The topology feature is available any time you are in the context of a target: select **Configuration** from the target type menu, then select **Topology**.
- Not all target types have configuration data. For these target types, the Configuration menu and topology graphs are not available.

26.10.5 Determining General Status of Target's Configuration Health

Topology enables you to view system health by displaying relationships among system entities, structure of a target, and target components, thus enabling you to analyze configuration health and status of the configuration.

Perform the following steps:

1. Access the Configuration Topology Viewer.

2. On the Configuration Topology Viewer page, icons indicate whether the target is down. You can choose a particular view, for example, Uses or Used By. In addition, icons indicate whether targets have associated incidents.

26.10.6 Getting Configuration Health/Compliance Score of a Target

To determine the configuration health and compliance score of a target, perform the following steps:

1. Access the Configuration Topology Viewer.
2. Zoom in on the target that has problems. Problems are represented by icons indicating a problem target status, and icons indicating target incidents. The target you selected in the All Targets page will always be highlighted.
3. When you hover over a target, click the **more** link in the popup. Properties for the target are available in the General, Incident Summary, and Configuration tabs. The Configuration tab shows information about target compliance, configuration changes in the past week, and recommended patches. Links from these values lead to more detailed reports.

If incidents are reported in the Incident Summary tab, resolve the reported events and incidents. Compliance information is available through the Configuration tab. If the target is not compliant, resolve the issue. Also if patches are missing, apply them.

4. Repeat the process of analyzing the various targets until all targets are functioning properly.

26.10.7 Analyzing a Problem and Viewing a Specific Issue in Detail

When you drill-down in topology graphs, you can have a detailed view of the specific issue that could be the cause of the problem.

Perform the following steps:

1. Access the Configuration Topology Viewer.

From the **Targets** menu on the Cloud Control home page, select **All Targets**. In the table, click the appropriate target. On the resulting page, select **Configuration** then select **Topology** from the dynamic target menu.

To view target data, place the mouse over the node and continue to move the mouse to >>. The popup containing data appears. Select **more** for additional information. The links associated with the data lead to the detail pages.

2. View configuration history changes.

From the dynamic target menu, select **Configuration**, then select **History**. On the Configuration History page, determine whether there has been a history change in the last 24 hours. If so, view those changes in detail for that particular target.

3. View compliance violations, incidents, and unauthorized changes.
4. View critical or warning incidents generated for a particular target.

From the **Enterprise** menu, select **Monitoring**, then select **Incident Manager**.

5. Determine whether there are patch recommendations.

On the Topology page, hover over an element and click **more** in the popup. Click the **Configuration** tab and determine whether Patch Advisories have been addressed.

26.10.8 About Dependency Analysis

Dependency analysis, also known as root cause analysis, traverses the relationships top to bottom to see if there is cause of a problem due to an issue with an asset on which the item is dependent.

To find the source of a target's health problem, perform the following steps:

1. Access the Configuration Topology Viewer.
2. In the **View** list, select **Uses**. This shows a topology of the targets that the selected target depends on.

Paths to the target or targets *potentially* causing the problem are colored.

If your target is not up, paths to the target or targets that may be causing the problem are colored. Red links lead from your target to targets that are down, and yellow links lead to targets whose status is not known.

By default the topology includes all depths of the tree, including the dependency relationships between those targets.

26.10.9 About Impact Analysis

Impact analysis traverses the relationships from the bottom to the top of the tree to see if a problem will occur if changes are made to the element (target or system) in which I'm interested. It answers the question: What items are dependent on my element that would be effected should I do something to my element. For example, if I shut down a listener, what databases would be affected?

Perform the following steps:

1. Access the Configuration Topology Viewer.
2. On the **Topology** page, analyze the **Used By** view. The topology will show the targets that depend on the selected target.

26.10.10 Creating a Custom Topology View

Create a custom topology view to include only those targets of interest, perhaps for a specific task or report. From a custom view, you can also augment the relationship data provided by Cloud Control.

Perform the following steps:

1. Access the Configuration Topology Viewer.
2. From the **Customize** menu, select **Create Custom View...** Provide the name and description for the topology and select one of the Initial Contents:
 - **Copy Current View** to create a topology view similar to the one you are viewing.
 - **Create Empty View** to create a topology view that starts with the root node.

Also, choose one of the following expose options:

- Expose the custom view for all targets of the current target type. For example, if you are creating a topology view for a database target, the new view will be available for all database targets.
- Expose the custom view for the current target only.

To share the view, click **Share this custom view with other users**.

Click **OK**.

3. Reduce the unwanted information in the topology by highlighting the target and selecting **Hide Relationships...** in the **Customize** menu.

You can also display relationships that are not being displayed by selecting a target. From the **Customize** menu, select **Target**, then select **Show More Relationships to Target Type....**

Privileged users can also choose to share their custom views with other users. To share a custom view, select the checkbox labeled **Share this custom view with other users**.

4. Click **OK**.

26.10.11 Deleting a Custom Topology View

When a custom topology view is no longer of use, delete it so it no longer clutters the View list. **Note:** System owned views cannot be deleted.

Perform the following steps:

1. Access the Configuration Topology Viewer.
2. From the **View** list, select the topology view you want to delete.
3. From the **Customize** menu, select **Delete Custom View...**
4. Click **Delete Custom View** in the confirmation popup.

26.10.12 Excluding Relationships from a Custom Topology View

After you create a topology view, you may want to remove some of the targets displayed in the custom view. Note that you cannot modify the out-of-box topology views: Uses, Used By, and System Members.

Perform the following steps:

1. Access the Configuration Topology Viewer.
2. From the **View** list, select the topology view you want to change then select the target.

Note: System created views cannot be modified.

3. From the **Customize** menu, select **Hide Relationships....**
4. The list of relationships that are displayed in the graph are listed in the Hide Relationships page. You can multi-select the relationships to exclude from the graph. Click **OK**.

26.10.13 Including Relationships to a Target in a Custom Topology View

After you create a topology view, you may find it necessary to include more relationships in the custom view. This will add targets to your custom view if they are related to the currently displayed targets using relationships you include.

Perform the following steps:

1. Access the Configuration Topology Viewer.
2. From the **View** list, select the custom topology view you own or have the privileges to change. System views such as Uses, Used By, and System Members cannot be modified.

3. Highlight a target from which to expand the topology. From the **Customize** menu, select **Target**, then select **Show More Relationships to Target Type...**
4. The resulting dialog shows a list of the relationships that the selected target type can participate in. Select the relationships of interest, and click **OK**. Any targets that are related to the selected target type using the selected relationships will be added to the topology view.

26.10.14 Creating a Relationship to a Target

In cases where you find that Cloud Control has incomplete information about your systems, you can create relationships between targets.

Note: Once new relationships are created, any topology showing the specified relationships and containing the targets will automatically show the new relationships.

Perform the following steps:

1. Access the Configuration Topology Viewer.
2. From the **View** list, select the topology view you want to change then select the target.
3. Select a target in the topology to be one end of the relationship.
4. On the Create Custom View page, provide a name and description, choose the initial contents, and determine how this custom view should be exposed. Click **OK**.
5. From the **Customize** menu, select **Target**, then select **Create Relationship to Target...**
6. On the **Create Relationship to Target** page, select the related target and the relationship between targets. Only relationships that the target type can participate in are shown in the list. Not all target types can be related to each other.

Note: Created relationships are independent of the view. You can see and use created relationships in other areas of Cloud Control, such as System templates, topology views, and configuration comparisons. Deleting a custom view will not delete the new relationship.

7. On the Confirmation page, click **Create**.

The related target will be added to the view.

26.10.15 Deleting a Relationship from a Target

If you have created a relationship between two targets, you may decide that the relationship no longer exists. Reflect this change by deleting extraneous relationships where appropriate. Note that once relationships are removed, they no longer show in any topology views.

Perform the following steps:

1. Access the Configuration Topology Viewer.
2. From the **View** list, select a custom view.
3. Select the link to the relationship you want to delete. You can either right click the node to view the context menu that allows you to delete the relationship or, from the **Customize** menu, select **Relationship**, then select **Delete Relationship...**

4. On the Confirmation page, click **Delete**.

Relationships are used in various places in Cloud Control, such as System templates, topology views, configuration comparisons, and so on. Deleting a relationship from this topology can impact these other areas.

If you create a relationship, you can later delete it by using the **Delete Relationship...** menu item.

26.10.16 Controlling the Appearance of Information on a Configuration Topology Graph

To control the way the targets are displayed in a custom topology, you can customize the tier in which a target type is shown, and you can group target types together.

The tier in which a target type is shown will affect its vertical or horizontal placement in the topology, depending on whether the layout is left-right or top-down.

To customize the appearance, perform the following steps:

1. Access the Configuration Topology Viewer.
2. Create or select an existing custom view.
3. To control highlighted paths to targets that are down, toggle the "Highlight 'Down' Root Cause" menu item.

When this menu item is selected and the root target is down, paths from the root node to other down targets are highlighted. By visually following the highlighted paths, you may determine which targets are causing the root target's down status.

Note: When this option is selected, you will not be able to group nodes together.

4. To manipulate tiers:
 - a. On the **Customize** menu, select **Select Tiers**.
 - b. Select either **Specify Tiers** or **Use Default Tiers**. If you choose to specify tiers, drag target types to their desired tier.
5. To turn the coloring of the links on and off, on the **Customize** menu, select **Highlight "Down" Root Cause**.
6. To group targets:
 - a. Select a link that represents one or more associations between the source and destination target types.
 - b. On the **Customize** menu, select **Relationship**, then select **Group Targets...**(Another way to select group targets is to right mouse click a link and select **Group Targets**.)

All matching associations are placed into group boxes.

Note: Grouping targets is not possible when "Highlight 'Down' Root Cause" is selected.

Managing Compliance

Compliance Management provides the ability to evaluate the compliance of targets and systems as they relate to business best practices for configuration, security, and storage. This is accomplished by defining, customizing, and managing compliance frameworks, compliance standards, and compliance standard rules. In addition, Compliance Management provides advice of how to change configuration to bring your targets and systems into compliance.

This chapter explains how Compliance Management verifies that applications in your enterprise comply with preestablished standards and how to manage the compliance structure. This chapter includes:

- [Overview of Compliance](#)
- [Evaluating Compliance](#)
- [Investigating Real-time Observations](#)
- [Configuring Compliance Management](#)
- [Real-time Monitoring Facets](#)

27.1 Overview of Compliance

The Compliance Management solution provides the tools to evaluate targets and systems for compliance with business best practices in terms of configuration, security, storage, and so on. In addition, Compliance Management provides the capability to define, customize, and manage the entities used to evaluate compliance.

The compliance solution:

- Automatically determines if targets and systems have valid configuration settings and whether they are exposed to configuration-related vulnerabilities.
- Advises how to change configurations to bring targets and systems into compliance with respect to best practices.
- Provides real-time monitoring of a target's files, processes, and users to let Oracle Enterprise Manager Cloud Control (Cloud Control) users know where configuration change or unauthorized action are taking place in their environment.
- Provides out-of-box compliance frameworks (PCI, for example) and compliance standards to map to compliance standard rules. This mapping makes it possible to visualize how out-of-compliance settings and actions will affect any compliance framework an organization follows.

- Provides a compliance-focused view of IT configuration and change that is suitable for Line of Business Owners, IT Managers, and Compliance Managers to refer to regularly to check on their organization's compliance coverage.

Before you start using the compliance features, there are a few basics you need to know. See the following for details:

- [Terminology Used in Compliance](#)
- [Accessing the Compliance Features](#)
- [Privileges and Roles Needed to Use the Compliance Features](#)

27.1.1 Terminology Used in Compliance

The following terms are used throughout this chapter when discussing the compliance feature:

- Compliance Framework

A compliance framework is an organized list of control areas that need to be followed for a company to stay in compliance in their industry. Enterprise Manager uses compliance frameworks as a foldering structure to map standards and rules to the control areas they affect. Compliance frameworks are hierarchical to allow for direct representation of these industry frameworks. A Compliance Framework can be used to represent a framework such as PCI.

A single framework control area maps to one or more compliance standards. The outcome of these compliance standard evaluations results in a score for the given framework area.

- Compliance Standard

A compliance standard is a collection of checks or rules that follow broadly accepted best practices. It is the Cloud Control representation of a compliance control that must be tested against some set of IT infrastructure to determine if the control is being followed. This ensures that IT infrastructure, applications, business services and processes are organized, configured, managed, and monitored properly. A compliance standard evaluation can provide information related to platform compatibility, known issues affecting other customers with similar configurations, security vulnerabilities, patch recommendations, and more. A compliance standard is also used to define where to perform real-time change monitoring.

A compliance standard is mapped to one or more compliance standard rules and is associated to one or more targets which should be evaluated.

- Compliance Standard Rule

A compliance standard rule is a specific test to determine if a configuration data change affects compliance. A compliance standard rule is mapped to one or more compliance standards.

Cloud Control has the following types of compliance standard rules.

- Repository Rule

Used to perform a check against any metric collection data in the Management Repository

- WebLogic Server Signature Rule

Used to check a WebLogic target to support best practice configurations.

- Real-time Monitoring Rule
 - Used to monitor actions to files, processes, and database entities in real-time as the changes occur. Also captures users logging in and logging out, and SU and SUDO activities.
- Compliance Standard Rule Folder
 - Compliance standard rule folders are hierarchical structures that contain compliance standard rules.
- Importance
 - Importance is a setting that the user can make when mapping compliance frameworks, standards, and rules. The importance is used to calculate the affect a compliance violation will have on the compliance score for that framework control area or compliance standard.
 - For compliance frameworks, when mapping a compliance standard, the importance for this compliance standard indicates the relative importance to other compliance standards in this framework.
 - For compliance standards, when mapping a compliance standard rule, importance indicates the relative importance of a compliance standard rule to all other compliance standard rules in the compliance standard.
- Score
 - A target's compliance score for a compliance standard is used to reflect the degree of the target's conformance with respect to the compliance standard. The compliance score is in the range of 0% to 100% inclusive. A compliance score of 100% indicates that a target fully complies with the compliance standard.
- Real-time Facets
 - The real-time monitoring rule definition includes facets that specify what is important to monitor for a given target type, target properties, and entity type. A facet is a collection of patterns that make up one attribute of a target type. For example, the networking configuration files for your operating system could be defined by one facet containing multiple file names or file patterns.
- Real-Time Observations
 - Observations are the actions that were seen on a host or target that were configured to be monitored through real-time monitoring rules. Each distinct user action results in one observation.
- Observation Audit Status
 - Every observation has an audit status that determines if the observation was authorized, or unauthorized, or neither (unaudited). The audit status can be set manually or automatically through the real-time monitoring compliance standard rule configuration.
- Observation Bundles
 - Single observations are not reported from the Management Agent to the server. They are instead bundled with other observations against the same target, rule, and user performing the action. Bundles help combine like observations and make it easier to manage the observations in Cloud Control.

27.1.2 Accessing the Compliance Features

To access the compliance features, navigate to the **Enterprise** menu, select **Compliance**, then select one of the following:

- Dashboard

The dashboard provides a very high level view of results that show how compliant or at risk your organization or your area is. The dashboard contains dials representing the compliance score for a selected framework, least compliant systems and targets, and unmanaged discovered hosts.

- Results

Compliance results include evaluation results and errors for compliance frameworks and compliance standards, as well as target compliance.

- Library

The Compliance Library page contains the entities used for defining standards. From the Compliance Library page you can manipulate compliance frameworks, compliance standards, compliance standard rules, and real-time monitoring facets.

Note: The real-time monitoring facets are only for real-time monitoring rules.

- Real-time Observations

Observations are the actions that were seen on a host or target that were configured to be monitored through real-time monitoring rules. Each distinct user action results in one observation. Observations are additionally bundled if there are multiple observations done in a short period of time by the same user on the same target and against the same real-time monitoring rule.

Multiple UI-based reports are provided to allow users to analyze the actions that are being observed.

27.1.3 Privileges and Roles Needed to Use the Compliance Features

To use the compliance standard features, you need to have access to the following privileges and roles.

Privilege	Description
CREATE_COMPLIANCE_ENTITY	Allows you to create compliance standards, compliance standard rules, and Real-time Monitoring facets
FULL_ANY_COMPLIANCE_ENTITY	Allows you to edit and delete compliance standards and compliance standard rules
VIEW_ANY_COMPLIANCE_FWK	Allows you to view compliance framework definition and results
MANAGE TARGET COMPLIANCE	Allows you to associate a compliance standard to a target
VIEW	Allows you to view a single target

Role	Description
EM_COMPLIANCE_DESIGNER	Using this role you can create, modify, and delete compliance standards, compliance standard rules, and Real-time Monitoring facets.
EM_COMPLIANCE_OFFICER	Using this role you can view compliance framework definitions and results.

The following table lists the compliance tasks with the privileges and roles required.

Task	Privileges and Roles Required
Create compliance framework	CREATE_COMPLIANCE_ENTITY privilege VIEW_ANY_COMPLIANCE_FWK privilege
Edit and delete compliance framework	FULL_ANY_COMPLIANCE_ENTITY privilege VIEW_ANY_COMPLIANCE_FWK privilege
Create, edit, and delete compliance framework	EM_COMPLIANCE_DESIGNER role EM_COMPLIANCE_OFFICER role
Associate a compliance standard to a target	MANAGE_TARGET_COMPLIANCE privilege
Import or export a compliance framework	EM_COMPLIANCE_DESIGNER role EM_COMPLIANCE_OFFICER role
Create a real-time monitoring rule	EM_COMPLIANCE_DESIGNER role
Create a real-time monitoring facet	EM_COMPLIANCE_DESIGNER role

In addition, ensure you have privileges to access the target you will be associating with a compliance standard. In particular, you need the Manage Target Compliance privilege on the target.

27.2 Evaluating Compliance

Compliance evaluation is the process of testing the compliance standard rules mapped to a compliance standard against a target and recording any violations in the Management Repository.

By evaluating a target against a compliance standard, you are determining whether a target complies with the checks of the standard. In the case when a target does not meet the desired state, the test may suggest what changes are required to make that target compliant.

Compliance evaluation generates a score for a target based on how much the target is compliant with the standard. A 100% compliance score means that all checks of the compliance standard passed on the target. For real-time monitoring, the compliance score will drop as you have observations that have been marked as unauthorized either manually or through change request management integration. As these unauthorized observations are either cleared or changed to authorized, the score will improve.

Because target compliance is required to be monitored regularly, you need to associate a compliance standard with targets. Evaluation is automatically performed for any associated targets, when the target state refreshes, that is when new data has been collected from the target. For repository rules, when new data for the target gets loaded into the Management Repository, evaluation happens again. For Real-time Monitoring, evaluation happens every time an observation of a user action is seen.

What You Can Do To Ensure Compliance

When using Cloud Control to evaluate your compliance, you should regularly perform the following actions:

- Regularly monitor the compliance dashboard to find areas that may indicate your organization has a low compliance score or is at risk
- View the results of an evaluation

Study the results of the evaluations and make the needed changes to the targets

Only results from the targets for which you have View privilege will be available. The compliance standard rule evaluation results are rolled up in order to produce a compliance standard evaluation state as well as a compliance summary.

- Study out-of-box reports

Regularly monitor real-time monitoring observation UI reports to see if detected observations are normal or abnormal. Set abnormal observations to unauthorized until any unauthorized change can be reverted or until the actions can be investigated to the level required by your auditors.

- Study the trend overview as a result of the evaluation

Use the graphs in the Trend Overview pages to visually determine whether the targets are adhering to or distancing themselves from the compliance best practices.

To access the Trend Overview pages for compliance standards:

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. From the **Compliance Standards** tab, choose **Evaluation Results**.
3. On the Evaluation Results page, choose the compliance standard you want to investigate and click **Show Details**.
4. On the resulting details page, click the **Trend Overview** tab.

Note: You can also review Trend Overview pages for compliance frameworks.

- Ensure your environments match baselines (or each other) by creating rules on top of configuration compare capabilities. Then monitor for configuration drift using real-time monitoring.
- Evaluate validity of configuration settings
- Evaluate exposure to configuration-related vulnerabilities, storage, and security
- Modify targets and systems to be compliant
- Verify authorization of configuration changes or user actions
- Continually test your systems, services, and targets, ensuring the best possible protection and performance your system can have
- Use out-of-box compliance standards and compliance standard rules to determine compliance. Click here to see a demo of this functionality.
- Keep an eye on hosts in your environment that are not monitored for compliance as these introduce a large amount of compliance risk in your environment.

The following sections provide additional details:

- [Accessing Compliance Statistics](#)
- [Viewing Compliance Summary Information](#)
- [Viewing Target Compliance Evaluation Results](#)
- [Viewing Compliance Framework Evaluation Results](#)
- [Investigating Compliance Violations and Evaluation Results](#)
- [Investigating Evaluation Errors](#)
- [Analyzing Compliance Reports](#)

- [Overview of Compliance Score and Importance](#)
- [Investigating Real-time Observations](#)

27.2.1 Accessing Compliance Statistics

Compliance statistics are available throughout the interface in Compliance Summary regions located on pages such as the Compliance Dashboard, the Enterprise Summary page, and a target's home page.

These regions report the violations and compliance scores for the particular targets. However, the region only reports that there is a violation; it does not give the details. For example, a violation can be against the Secure Port compliance standard rule that is part of the Secure Configuration for Host compliance standard. But you will not know the details just by looking at the Compliance Summary regions.

27.2.1.1 Using the Compliance Dashboard Effectively

The compliance dashboard is a top level view of the Cloud Control compliance features. The dashboard includes several regions which give you a very good insight into how compliant your IT environment is according to the standards you have configured.

To access the Compliance Dashboard:

1. From the Enterprise menu, select **Compliance**.
2. Select **Dashboard**.

The Compliance Dashboard is also one of the pages available from the "Select Your Home" page and can be set as your home page when you log in to Cloud Control.

The Compliance Dashboard includes the following regions:

- **Compliance Framework Summary**

This region lets the user choose one Compliance Framework and it shows the compliance score for each second-level folder under that Compliance Framework. Each dial has two needles. One represents the current compliance score (the thicker one) and the other represents the lowest score seen in the last seven days. Between these two needles, it is possible to tell if the compliance score is improving or is recently at its low point. If the two needles are at the same level, this shows you that right now the score is around the lowest it has been for the last seven days. If the current score is much better than the last seven days needle, this shows you the score has improved recently.

Clicking on one of the dials will take you to the Compliance Results page for the given second-level framework folder giving you more details on the next framework folders down and/or the compliance standards belonging to this folder.

- **Compliance Summary**

This region has a view for frameworks and a view for standards. In the Framework view, this region shows you the list of all defined compliance frameworks and their overall score and violation details. In the standard view, this region will list the worst scoring compliance standards along with their violation details. Clicking on a framework or standard name will take you to a screen showing you more details of that framework or standard.

From this region, you can also click on the View Trends link to see a historic trend graph of the compliance score

- **Least Compliant Generic Systems**

This region shows the generic systems that have the lowest compliance score. The score for a given system is calculated by including all rules that are associated with all elements of that system. A generic system is used to define your IT Business Applications, such as HRIS, Payroll, and so on. Reporting these systems that have the lowest score can help identify which business units have compliance risk leading up to audit time.
- **Most Recent Discovered Unmanaged Hosts**

This region shows hosts that have been discovered recently using the Cloud Control automatic host discovery feature that have not been promoted to managed hosts. These hosts represent a specific compliance risk in that unmanaged hosts in an IT environment can be lead to many access control and data access risks. The intent of this region is to highlight the hosts that have recently been discovered but may not be under compliance control.
- **Least Compliant Targets**

This region is similar to the Least Compliance Generic Systems except it shows you all targets (including the generic systems again). This region is less useful for an IT management or auditor perspective since it may not be clear what these individual targets are used for. It however can be used as another data point to find the areas where you are at highest risk leading up to an IT compliance audit.

27.2.2 Viewing Compliance Summary Information

Compliance summary information is available from the Cloud Control Compliance Results page and individual target home pages.

To view compliance summary information from the Cloud Control home page, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.

To view compliance summary information from a target's home page, follow these steps:

1. From the **Targets** menu, select the target type, and click the target.
2. On the target's home page, scroll down to the **Compliance Standards Summary** region.

To view compliance summary information from the target menu on a target's home page, follow these steps:

1. From the **Targets** menu, select the target type, and click the target.
2. On the target's home page, click the target menu located at the top-left of the page.
3. Select **Compliance**, then select **Results**. On the Results page, click **Target Compliance**.

27.2.3 Viewing Target Compliance Evaluation Results

Target-specific compliance evaluation results are available on the Cloud Control home page and individual target home pages. By evaluating compliance rules and standards, the possible evaluation results will be:

Evaluation Results	Description
Compliant	Target meets the desired state and there are no unauthorized real-time monitoring observations.
Non-Compliant	Target does not meet the desired state. At least one test in the compliance standard detected a deviation from the desired state or there is at least one unauthorized real-time monitoring observation.
Error	<p>No results returned due to an error. The error may be an unexpected internal error or an error in the test. Examples of errors in the test include attempts to:</p> <ul style="list-style-type: none"> ▪ Divide by zero ▪ Invoke a function with incorrect parameter values

To view results using Cloud Control home page, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. Click the **Target Compliance** tab. The Target Results page displays the targets with their Average Compliance Score.

To view compliance evaluation results from a target's home page, follow these steps:

1. From the **Enterprise** menu, select **Targets**, then select the target type.
2. Click the name of the target in which you are interested.
3. On the target's home page, scroll to the **Compliance Standard Summary** region.

Use the page or region to get a comprehensive view about a target in regards to compliance over a period of time. Using the tables and graphs, you can easily watch for trends in progress and changes.

Note: Trend overview data might take up to six hours after initial compliance standard to target association to display in the time series charts.

27.2.4 Viewing Compliance Framework Evaluation Results

To effectively use a compliance framework, organize the frameworks to reflect the compliance framework control areas you use in your organization. The hierarchical structure of the framework should map directly to the control areas of the frameworks you follow.

Oracle provides an out-of-box framework for Payment Card Industry (PCI), as well as one for the Oracle Generic Compliance. These out-of-box frameworks can be used as a starting point for you to create your own frameworks to match your needs or can be used to understand how best to organize your own frameworks based on internal standards or based on SOX, HIPAA, NIST-800, or other common frameworks.

To view the results of a compliance framework evaluation, use the Evaluations Results page accessed through the Compliance Frameworks tab.

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. On the Compliance Results page, click the **Compliance Frameworks** tab and highlight the compliance framework of interest.

Since compliance frameworks are a hierarchical structure, each folder or node of the framework will have its own score. The bottom most children of the hierarchy will have their score roll up to the parent folder and so on. If one person viewing these reports is primarily interested in one control area of the framework they follow, they

can focus on the score for that specific control area as represented by the folder they look at under the framework.

For example, in the PCI framework, there are second level folders for Network Configuration separate from Access Control. If there are violations in network configuration, these would only be visible in the Network Configuration folder's score and the top level PCI score would also be affected.

27.2.5 Investigating Compliance Violations and Evaluation Results

Here are a few suggestions for investigating compliance violations. Attend to the most critical violations or those that have the biggest impact on your overall IT enterprise compliance.

- Monitor the compliance framework scores along with the systems and targets that have the lowest scores on the compliance dashboard.
- Ensure that recently discovered hosts are either being monitored using Cloud control for compliance risk or are not possibly introducing risk in your IT compliance.
- Study the statistics on the Enterprise Summary Home page. In particular, look at the statistics in the Compliance Summary region. The compliance violations with "Critical" severity should be dealt with first.
- Address generic systems (IT business applications) and targets that have the lowest compliance scores.
- For the compliance violations of a particular target, examine the home page for that target. The Compliance Standard Summary region provides overview information, but it also gives you access to the Trend for that target.
- Review compliance violation-related events in the Incident Management area of Cloud Control.
- Navigate to the Results page for a particular compliance standard. In the navigation tree, click the name of the compliance standard and a summary page lists all the targets along with the number of violations.
- Navigate to the Trend Overview page to see charts relating to the number of targets evaluated, the average violation count per target, number of targets by compliance score, and the average compliance score.

Note: Only results from those targets for which you have View privilege will be available for viewing.

27.2.5.1 Investigating Violations of Repository Compliance Standard Rules and Targets Causing Violations

If you are looking at the Enterprise Summary page and you notice that there are critical violations against the Secure Configuration for Host compliance standard, you need to find what targets are causing the violations. Follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. In the Evaluations Results tab for Compliance Standards, highlight the Secure Configuration for Host compliance standard. Click **Show Details**.
3. In the Summary tab on the Compliance Standard Result Detail page, you can look at the results either by target or compliance standard rule. For this example, we will use Result by Compliance Standard Rule.

4. In the navigational list, click the **Secure Ports** compliance standard rule. In the resulting Secure Ports Summary tab, you will get a list of all the targets that are violating the Secure Ports rule. This is a security issue that needs to be addressed.

27.2.5.2 Viewing All the Violations Reported for Your Enterprise

If you want to see all the targets that are not compliant with the compliance standards:

- From the Enterprise menu, select **Compliance**, then select **Results**.
You have the option of viewing violations associated with compliance standards and compliance frameworks.
 - Click the **Target Compliance** tab for a roll-up view of all violations across all targets, that is, all those targets that are out of compliance.
 - Click the **Compliance Standards** tab to view the list of compliance standards against which there are violations. From this tab, you can also access the Errors tab to view the errors against the compliance standard.
- Navigate to the Home page for a particular target. The Compliance Standard Summary region lists the compliance violations according to severity level. Click the name of the compliance standard of interest to view the details of the violations.

27.2.5.3 Examples of Viewing Violations

As noted in the previous sections, the compliance feature provides violation details that help you resolve compliance issues. There are a number of ways to access violation details.

Violations are available from the following:

- **Compliance Summary** region located on the Enterprise Summary page.
You can easily see the violations against compliance frameworks and compliance standards.
- Compliance Results page. From the **Enterprise** menu, select **Compliance**, then select **Results**.

The following are examples of how to find violation details.

Example 1 - Accessing Violation Details of a Compliance Framework

To see the violations of a compliance framework, click the **Compliance Frameworks** tab then the **Evaluation Results** tab. The Violations columns list how many violations exist for each framework. When you click the number in a Violations column, all the targets with their associated compliance standards are listed.

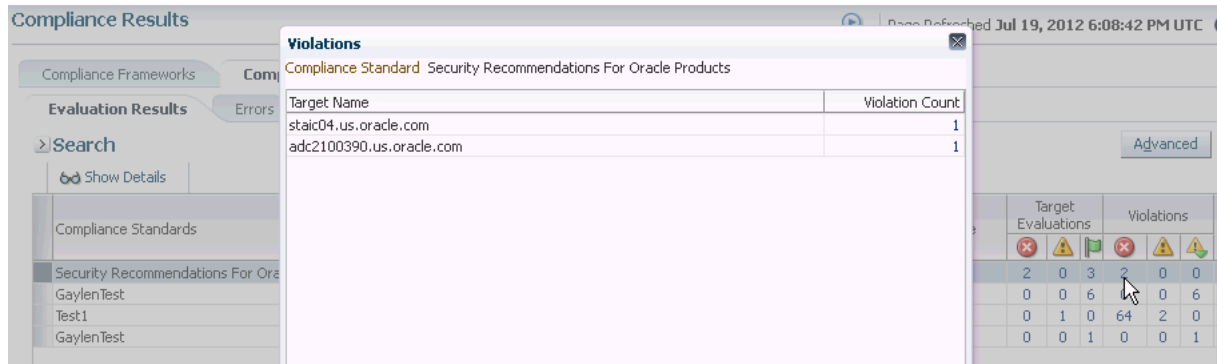
In turn, when you click the number in the Violation Count column, the resulting Violations page lists the compliance standard rule that is violated. Again when you click the number in the Violation Count column, the resulting Violation Details page lists all metrics for a particular compliance standard rule that are responsible for the violations.

Example 2 - Accessing Violation Details of a Compliance Standard

When you click the **Compliance Standards** tab then the **Evaluation Results** tab, the Violations columns report how many violations exist for each compliance standard.

When you click the number in a Violations column, the Violations pop-up appears listing all the targets violating the standard. See [Figure 27-1](#).

Figure 27–1 Violations for a Compliance Standard



Again, click the number in the Violation Count column and the Violations pop-up appears. All the Compliance Standard Rules, for example Security Recommendations, are listed.

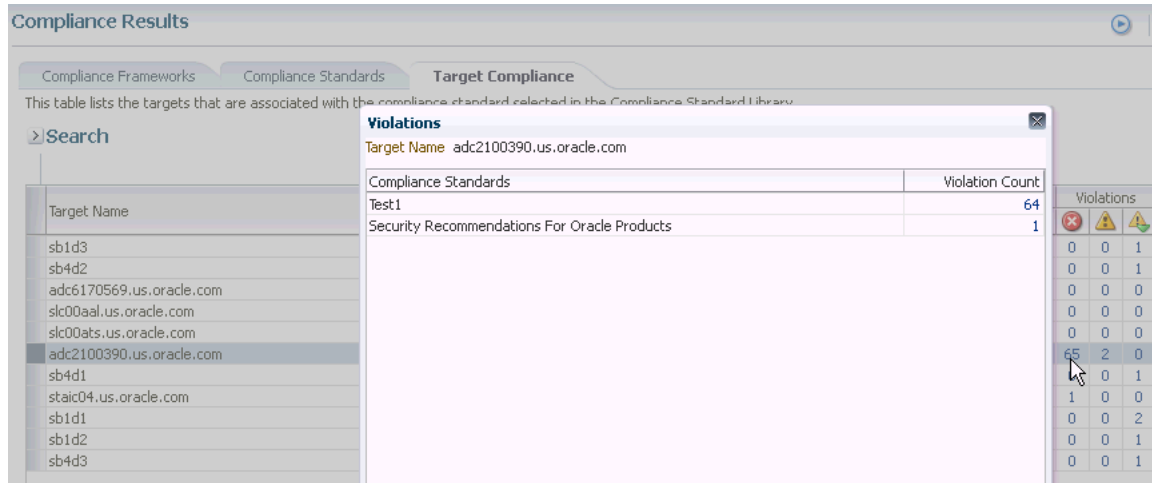
You continue the process by clicking the number in the Violation Count column again in the Violations pop-up. The subsequent pop-up displays the Violations Details. For example, the Violations Details pop-up displays the name of the patch that is causing the problem.

Example 3 - Accessing Violations of a Target

When you click the **Target Compliance** tab, the Violations columns report how many violations exist for each target.

When you click the number in a Violations column, the Violations pop-up appears listing all the targets violating the standard. See [Figure 27–2](#).

Figure 27–2 Violations Using the Target Compliance Tab



Again, click the number in the Violation Count column and the Violations pop-up appears. All the Compliance Standard Rules, for example Security Ports, are listed.

You continue the process by clicking the number in the Violation Count column again in the Violations pop-up. The subsequent pop-up displays Violations Details. For example, the Violations Details pop-up displays the numbers of the ports violating the compliance standard.

Example 4 - Violations Using Show Details on Compliance Standards Page

You can also drill-down on violations using the Show Details option on the Compliance Results page. Highlight a standard and click **Show Details**. See [Figure 27-3](#).

Figure 27-3 Show Details Page

The screenshot shows the 'Compliance Results' page with tabs for 'Compliance Frameworks', 'Compliance Standards', and 'Target Compliance'. Under 'Compliance Standards', there are sub-tabs for 'Evaluation Results' and 'Errors'. A search bar is visible with a 'Show Details' button highlighted. Below the search bar is a table with columns: 'Compliance Standards', 'Applicable To', 'Compliance Standard State', 'Target Evaluations', and 'Violations'. The first row shows 'Security Recommendations For Oracle Products' applicable to 'Host' in 'Production' state, with 2 target evaluations and 2 violations.

Compliance Standards	Applicable To	Compliance Standard State	Target Evaluations	Violations
Security Recommendations For Oracle Products	Host	Production	2 0 3	2 0 0

On the resulting page, you have the option of seeing violations by target or by compliance standard rule.

When you click the **Violations** tab, details regarding the compliance standard are listed including Event Details and Guided Resolution. See [Figure 27-4](#).

Figure 27-4 Event Details and Guided Resolution

The screenshot shows the 'Security Recommendations For Oracle Products (Compliance Standards)' page with the 'Violations' tab selected. A table lists violations with columns: Rule, Target Name, Applicable To, Severity, Keywords, and Recommendation. Below the table, a specific violation is highlighted: 'The target db112.us.oracle.com in host adc2100390.us.oracle.com is vulnerable. The security patch 14,038,787 is applic...'. The page is divided into two main sections: 'Event Details' and 'Guided Resolution'. 'Event Details' shows metadata like Root Compliance Standard, Rule Name, and Target. 'Guided Resolution' provides recommendations, diagnostics, and actions for resolving the issue.

Rule	Target Name	Applicable To	Severity	Keywords	Recommendation
Security Recommend: adc2100390.us.oracle.com Host		Host	Critical	Configuration, Security	Apply one of the identified security patches to the corresponding target in
Security Recommend: staic04.us.oracle.com Host		Host	Critical	Configuration, Security	Apply one of the identified security patches to the corresponding target in

Event Details

- Root Compliance Standard: Security Recommendations For Oracle Products
- Root Compliance Standard Author: ORACLE
- Root Compliance Standard Version: 1
- Rule Name: Security Recommendations
- Rule Type: Repository
- Target: adc2100390.us.oracle.com (Host)
- Event Reported: Jul 17, 2012 7:05:46 PM GMT

Guided Resolution

Recommendations
Apply one of the identified security patches to the corresponding target in your host.

Diagnostics
View topology
View recent configuration changes

Actions
Disable rule for this target

- This event will be automatically cleared when the underlying issue is resolved.
- To stop repeat notifications, create an incident for this event and acknowledge it.

Example 5: Accessing Violations from Enterprise Summary Page

When you click the name of a compliance standard in the Compliance Summary region of the Enterprise Summary page, the Compliance Standard Result Detail page appears. By clicking the Violations tab, you can view all the targets that violate the particular compliance standard. See [Figure 27-5](#).

Figure 27–5 Compliance Summary Region on Enterprise Summary Page

Compliance Summary

Compliance Frameworks Compliance Standards

View Trends

Name	Target Evaluations			Violations			Average Compliance Score (%)
	✖	⚠	✔	✖	⚠	✔	
Test1	0	1	0	64	2	0	67
Security Recommendations For Oracle Products	2	0	3	2	0	0	80
GaylenTest	0	0	1	0	0	1	99
GaylenTest	0	0	6	0	0	6	99

On the Compliance Standard Result Detail page, when you click the Summary tab then the Result By Target tab, the number of violations against the target display. When you click a number in the violations columns, the Violations pop-up appears listing the compliance standard rules that are causing the violation. In turn, when you click the number in the Violation Count column, the name of the offending metric or patch displays.

Note: Similar drill-downs are available from the Target Compliance tab.

Tip: To get to the end result of a Violation, continue clicking the number in the Violation Count column. More and more details are presented, narrowing the cause of the problem.

27.2.6 Investigating Evaluation Errors

The Evaluation Errors page reports statistics about the problems encountered during the evaluation. On initial display, the Evaluation Errors page shows all the evaluation errors.

- Use the Evaluation Errors page to view the errors that occurred as a result of metric collection, as well as those that occurred during the last evaluation.
- Use the search filter to view only those evaluation errors that meet a set of search criteria that you specify.
- Click the message in the Message column to decide what your course of action should be to resolve the error.
- Normally the results of an evaluation overwrite the previous evaluation's results. However, in the case of evaluation failure or data provider collection failure, the previous results are left untouched.

Once the underlying problem is fixed, the error will no longer be reported.

Search Filter for Evaluation Errors

By default, all the evaluation errors in your enterprise configuration appear in the results table. However, you can specify a set of search criteria and then perform a search that will display only the evaluation errors that meet those criteria in the results table.

For example, if you choose Host in the Target Type list, contains in the Target Name list, and "-sun" in the adjacent Target Name text field, and then click **Go**, Cloud Control displays, in the results table, only the compliance standard rule evaluation errors for the hosts that contain "-sun" in their names.

27.2.7 Analyzing Compliance Reports

Cloud Control provides reports specific to compliance. To access these reports:

1. From the **Enterprise** menu, select **Reports**, then select **Information Publisher Reports**.
2. Scroll to the Compliance section

Compliance reports include the following:

- Descriptions reports

The Descriptions reports list all the available compliance standards, compliance frameworks, and compliance standard rules available in the Compliance Library. These reports enable you to decide whether additional compliance standards and compliance frameworks need to be defined for your enterprise to attain and maintain its compliance to the standards.

- Results reports

The Results reports provide details of the various evaluations against compliance standards and compliance frameworks. Using the Results reports you can view, in one place, all the statistics regarding the compliance of your enterprise against the defined standards. To view the target that is most likely in need of your immediate attention, view the Target with Lowest AVG COMPLIANCE SCORE report. The following are examples of the reports provided:

- Compliance Standard Results Details

Displays the compliance summary for all the compliance standards evaluated against a target. Data includes compliance score, compliant and non-compliant rules, violations, and last evaluation date.

- Compliance Standard Result Summary

Displays the compliance summary of a particular compliance standard. For example, if there are three targets each reporting on Security Recommendations for Oracle Products compliance, the Result Summary rolls up the information into one report. Data includes average compliance score, the number of targets that need immediate attention, and the number of rules that are non-compliant.

Cloud control also provides a set of reports using the new BI Publisher integration. The following reports are available:

- Real-time Monitoring Violation Report

Shows current violations based on real-time monitoring rule type.

- Compliance Summary Report

Shows current compliance score, compliance trends, top 10 least compliant system targets and framework violation summary for a specific Compliance framework and all second-level framework folders.

- Observation Journal Report

Tabular report showing observations that have occurred over a period of time. The user can choose which targets and the start and end time for the report.

Note: To enable BI Publisher reports that include Compliance Frameworks to function, the user running the reports must have the EM_COMPLIANCE_OFFICER role.

27.2.8 Overview of Compliance Score and Importance

A target's compliance score for a compliance standard is used to reflect the degree of the target's conformance with respect to compliance standard. The compliance score is in the range of 0% to 100% inclusive. A compliance score of 100% indicates a target fully complies with the compliance standard.

During an evaluation, a target is found to be compliant or non-compliant with that compliance standard.

Types of Importance

Importance is a setting that the user can make when mapping compliance frameworks, standards, and rules. The importance is used to calculate the affect a compliance violation will have on the compliance score for that framework control area or compliance standard.

For compliance frameworks, when mapping a compliance standard, the importance for this compliance standard indicates the relative importance to other compliance standards in this framework.

For compliance standards, when mapping a compliance standard rule, importance indicates the relative importance of a compliance standard rule to all other compliance standard rules in the compliance standard.

However, just because a compliance standard rule has an importance of 'low' does not mean that it can safely be ignored. All compliance violations should be triaged and cleared once the risk has been removed through a fix or a compensating control.

Importance is used to weight compliance scores as they roll up in a compliance standard hierarchy.

The following sections provide examples of how the compliance score is calculated.

27.2.8.1 Compliance Score of a Compliance Standard Rule -Target

Note: This calculation is used for WebLogic Server Signature rules and Repository rules.

Compliance score of a compliance standard rule-target is calculated by taking the severity and importance of the compliance standard rule and multiplying the result by the total number of violations divided by the total number of rows evaluated for that target.

The formula is:

$$\text{hirange} - (\text{hirange} - \text{lorange}) * (\text{number of violations} / \text{number of rows evaluated})$$

The following table provides the combination of the severity and importance values used to calculate a compliance score.

Table 27–1 Importance and Severity Ranges

Importance	Critical Severity (1)	Warning Severity (1)	Minor Warning Severity (1)
High	0-25 (2)	66-75	95-96
Normal	26-50	76-85	97-98
Low	51-75	86-95	99-99

(1) low range and high range of the severity

(2) 0 is the lorange; 25 is the hirange

27.2.8.2 Real-time Monitoring Rule Compliance Score

The compliance score of a real-time monitoring rule is based on the number of observation bundles that have violations compared to how many observation bundles there have been over time. An observation bundle is a collection of all observations that happen over a short period of time (few minutes) by the same user against the same target. For instance, if user A is logged into a host and makes 10 file changes in 5 minutes. These 10 observations will all belong to the same bundle. The bundling is handled automatically by Enterprise Manager.

When calculating the count of past observation bundles, the most recent bundles are weighted higher and they have a different weighting as they get older.

The score is calculated using the formula:

$$1 - V/T$$

where T is the sum of all the weighted bundle counts
and V is the count of the current bundles in violation

The result of the calculation of $1 - V/T$ will be a number around 1 as V is 0 (100% compliant) or will be a number near 0 when V is close to the value of T (0% compliant).

27.2.8.3 Compliance Score of a Compliance Standard for a Target

The compliance score of a compliance standard for each target is calculated by taking the individual compliance score of each rule - target and multiplying it by its importance. This multiplication is repeated for each rule then the resulting products are added. The sum of the products is then divided by the sum of the importance of each rule. See [Figure 27-6](#).

Figure 27-6 How Compliance Score of a Compliance Standard-Target Is Calculated

Key:

CS: compliance standard

Rule: compliance standard rule. There are 3 rules: Rule1, Rule2, and Rule3.

i: importance

i1: importance for Rule1

i2: importance for Rule2

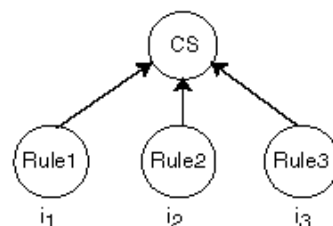
i3: importance for Rule3

S: compliance score of the rule

S1: compliance score for rule1-target

S2: compliance score for rule2-target

S3: compliance score for rule3-target



$$\text{Compliance Score of Compliance Standard-Target} = \frac{(S_1 \times i_1) + (S_2 \times i_2) + (S_3 \times i_3)}{(i_1 + i_2 + i_3)}$$

27.2.8.4 Compliance Framework Compliance Score

The compliance framework score is a rolled up weighted average of all compliance standard-target scores across all compliance standards within the compliance framework hierarchy. The weight is based on the importance of a compliance standard. In [Figure 27-7](#), compliance framework CF has 2 standards CS1 and CS2. CS1 is associated and evaluated on targets t1 and t2 and CS2 is associated and evaluated on targets t3 and t4.

Figure 27-7 How Compliance Score of a Compliance Framework Is Calculated

Key:

CF: compliance framework

CS: compliance standard

CS₁: compliance standard 1

CS₂: compliance standard 2

t: target

i: importance

i_{cs1}: importance of CS1

i_{cs2}: importance of CS2

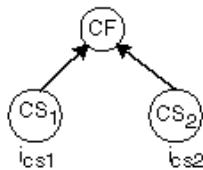
ST: compliance score of a compliance standard for a target

ST₁: compliance standard score for CS1-t1

ST₂: compliance standard score for CS1-t2

ST₃: compliance standard score for CS2-t3

ST₄: compliance standard score for CS2-t4



$$\text{Compliance Score of Compliance Framework} = \frac{(ST_1 \times i_{cs1}) + (ST_2 \times i_{cs1}) + (ST_3 \times i_{cs2}) + (ST_4 \times i_{cs2})}{(i_{cs1} + i_{cs1} + i_{cs2} + i_{cs2})}$$

27.2.8.5 Parent Node Compliance Score

The compliance score of a hierarchy node/parent node is calculated as shown in [Figure 27-8](#). Compliance standards are hierarchical, thus the top node in the tree is known as the parent node.

Figure 27-8 Compliance Score of Parent Node

$$\text{Compliance Score of Parent} = \frac{\sum_{\forall i} S_i \times I_i}{\sum_{\forall i} I_i}$$

In [Figure 27-8](#):

- *i* represents the number of children
- *S* is the score of the child node
- *I* is the importance of the child node

27.3 Investigating Real-time Observations

As previously described, observations are the actions that were seen on a host or target that were configured to be monitored through real-time monitoring rules. Each distinct user action results in one observation.

Observations can have one of many audit statuses. The basic audit status "unaudited" means that the observation was detected, there just is no indication that this action was good or bad. The authorized status means that some review has happened for the observation and it should be treated as expected to occur (it was a good change). The unauthorized status means that this observation has been reviewed and has been found to be against policy. This may result in either a corrective fix, a change to policy, or a compensating control being put in place. The audit status for observations can be automatically set by a rule so that all observations triggered by the rule get a default audit status. The status can also be set manually through the UI reports discussed below. The most advanced capability involves integrating with a Change Management Request server through a Cloud Control connector to automatically determine on a per-observation basis if that action was supposed to happen.

The following sections provide additional details regarding real-time monitoring observations:

- [Viewing Observations](#)
- [Operations on Observations During Compliance Evaluation](#)

27.3.1 Viewing Observations

There are 4 key ways to see what real-time monitoring observations have occurred in your environment:

- [Viewing Observations By Systems](#)
- [Viewing Observations By Compliance Framework](#)
- [Viewing Observations By Search](#)
- [Viewing Details of an Incident](#)

The first three observation screens are available from the Enterprise menu by selecting **Compliance**, then selecting **Real-time Observations**. This page that lets you choose which of the three reports to look at and also shows any Management Agent warnings related to configuration of Real-time monitoring rule configuration. These warnings are reported from the Management Agent and could impact observations from being delivered to the Cloud Control server. If you are missing observations that are expected, review these warnings and address any configuration issues that is causing them.

27.3.1.1 Viewing Observations By Systems

When observations occur, they can be marked as authorized or unauthorized automatically. This provides one way you to find observations that are important for you to look into. However, if a rule is not configured to reconcile observations with a change management server, it can be difficult to find the observations that are important to you through only an attribute search. Being able to view observations by business application (generic systems) and drilling down into observation details allows you to discover where there may be issues that should be investigated regardless of the observation's audit status.

Typically, IT managers and line of business owners must identify when unwanted configuration drift occurs in their business applications. By browsing observations by

systems, you can easily see which changes affect specific business applications. Observations can be filtered by whether they are authorized, unauthorized, unaudited or both. They can also be filtered by time.

This begins with you choosing one or more business applications and being able to see the relative counts of observations. This report starts at the business application level (generic systems) because an IT manager and compliance auditor may not know what a target is used for. A business application is modeled in Cloud Control as a generic system.

If you are more technical, you still may want to start at this business application level if this is the business application you are working on.

To view observations by systems, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Real-time Observations**.
2. Click **Browse Observations by System Targets**.

Cloud Control displays the Select Root Target(s) page that lists the Target Name for each system target. There is also a link for all targets not belonging to a system target.

3. You can begin viewing a report for a given system target by selecting one or more system targets and clicking on the View Details for Selected Systems button.

You will see counts for each system target selected by the time range selected. For instance if you are looking at the monthly time range, each column in the table will represent one day from the month. The count will be the count of observations for that day and system target.

Click on the system target name to drill down and show the counts by each target that comprises the system target. You can continue to click on the links in the first column of the table to drill down until you get to the entities that had observations (for example: file names, process names, user accounts, and so on).

Clicking on the count displays a screen that shows the actual observations that occurred during that time period.

27.3.1.2 Viewing Observations By Compliance Framework

The ability to view observations as they relate to a compliance standard structure is something that is typically done by a non-technical role such as an IT Manager, Line of Business Owner, Compliance Manager, or Executive.

You can identify some set of Compliance Frameworks that reflect the IT compliance framework that the organization follows. Observations can be filtered by whether they are authorized, unauthorized, unaudited or both. They can also be filtered by time.

To view observations by Compliance Framework, follow these steps:

1. From the Enterprise menu, select **Compliance**, then select **Real-time Observations**.

Clicking on the count displays a screen that shows the actual observations that occurred during that time period.

2. Click **Browse Observations by Compliance Frameworks**.

Cloud Control displays the Select Compliance Frameworks page that lists each defined Compliance Framework.

3. You can begin viewing a report for a given framework by selecting one or more frameworks and clicking on the View Details for Selected Frameworks button.

You will see counts for each framework selected by the time range selected. For instance if you are looking at the monthly time range, each column in the table will represent one day from the month. The count will be the count of observations for that day and framework.

Click on the framework name to drill down and show the counts by each second-level framework folder that is in the selected framework. You can continue to click on the links in the first column of the table to drill down until you get to the entities that had observations (for example: file names, process names, user accounts, and so on).

4. Clicking on the count displays a screen that shows the actual observations that occurred during that time period.

This drill-down capability provided by these screens makes it easy for you to easily find where observations are occurring. When you have an environment with tens of thousands of targets across hundreds of business applications, it is impossible to view observations simply using a table and search unless you know exactly the search conditions they are looking for. In a matter of an hour, with this large of an environment even with little activity, there can be thousands of observations.

27.3.1.3 Viewing Observations By Search

For cases when the two browse by screens cannot provide the best view of what observations have happened in your environment, Cloud Control also provides a search capability to find observations.

To search observations, follow these steps:

1. From the Enterprise menu, select **Compliance**, then select **Real-time Observations**.
2. Click **Search Observations**.

Cloud Control displays the Search observation page which has search filters on the top half of the page and search results on the bottom half

3. You can set any number of filters in the search area. You can also click on the Add Fields button to add any fields that are available in the search results table.
4. With the options available in search, you can find observations performed over a time range, by a specific user, against a specific target, changes to a specific entity, and so on. Nearly every use case for finding observations can be solved using a combination of search fields.

27.3.1.4 Viewing Details of an Incident

Observations are logically bundled together based on the compliance standard rule, target and user that performed the action. This bundling is discussed in more detail in Creating a Real-time monitoring Rule section.

When one or more observations of a bundle are unauthorized, the bundle is considered to be in violation. This violation will lead to an event being created in Cloud Control Incident Management. The event name will be based on the message field defined in the real-time monitoring rule. When viewing this event in the incident management UI, several fields will show details of the bundle; the target type, entity type, number of observations in the bundle, observations by audit status, and so on. You can click on the Update Audit Status link to go to the bundle observations page.

This Observations page shows the list of observations in the observation bundle for this event. You can filter on various attributes for each observation, including but not limited to the authorized/unauthorized status, user, time, and so on.

27.3.2 Operations on Observations During Compliance Evaluation

The following sections describe how a real-time monitoring observation's audit status can be adjusted and how notifications can help in evaluating compliance results.

[Manually Setting an Observation As Authorized Or Not Authorized](#)

[Notifying a User When an Observation Occurs](#)

[Notifying a User When an Authorized Observation Occurs](#)

27.3.2.1 Manually Setting an Observation As Authorized Or Not Authorized

Any time a user is viewing the details of a real-time observation, the user can change the audit status for the observation. You can override the audit status of an observation if you investigate the user action and determine that the activity should have resulted in a different audit status. Based on the real-time monitoring rule, all observations will either have a pre-set audit status or will have an audit status determined by an integration with a Change Request Management server. The available audit statuses are:

- **Unaudited:** No evaluation has happened to determine if the observation was good or bad.
- **Authorized:** The observation has been determined to be good, some action that was desired to occur.
- **Unauthorized:** The observation has been determined to be bad, some action that was not wanted.
- **Unauthorized-Cleared:** The observation had previously been determined to be bad, some action that was not wanted, but it has been handled through a fix, a policy change, or a compensating control and has now been cleared

To change the audit status of an observation, view the observation from either of the browse by UI pages, the observation search page, or the incident manager UI. Select the observation and click Update Audit Status. A popup will come up allowing you to select the new audit status and a comment describing the reason for the status change. The history of all audit status changes is maintained for each observation.

If the Cloud Control instance is using the Change Request Management server connector for integration, there are some special considerations:

If you change an unauthorized observation into an authorized observation, then you have the option of entering a change request ID that is known to authorize the change. This change request ID should match a request that already exists in your change request management system. You can also enter a comment. If a change request ID is provided, then the change request is annotated with the change just as if the system had automatically authorized it. If an incident had been created for the observation bundle, then the event/incident is updated with the new number of unauthorized observations.

If you change an authorized observation into an unauthorized or unaudited observation, any annotations that were made to any change requests are rolled back. If there was already an incident raised for the observation bundle, then the annotation is changed to update the number of unauthorized observations in the incident. If this is

the first unauthorized observation in a group, then an event is created an incident is raised. You can provide a comment for the change.

When you manually set the observation to be authorized and enter a change request ID and the rule has change management integration enabled, no attributes of the change request are compared with the observation. The change request is simply updated with the observation details.

When rolling back annotations in the change management server, the observation annotations are marked as rolled-back instead of actually removing the annotation. This occurs to avoid user confusion not knowing possibly why the annotations were removed. Also, if the observation later becomes authorized again, the rolled-back marking can simply be removed to bring the annotation back.

27.3.2.2 Notifying a User When an Observation Occurs

If a compliance standard rule is created and you do not use change management reconciliation with the rule, then there will be no automated authorized/unauthorized check done on the observations. You can specify for this rule that each observation bundle should result in informational event being generated for the observation bundle. Details on how to configure this is in the section [Creating a Real-time Monitoring rule](#).

The event will have a notation. From the Incident Management console the user can look at events and incidents. When looking at a single event, there is a link available to see the observations associated with this observation bundle's event. Each observation bundle can only have one event. If at least one observation in the bundle is unauthorized, then the bundle is considered to be in violation which results in the event being generated.

Since this notification does not require user intervention or follow-up action, it is treated as informational. If at a later time, someone changes one of these unaudited observations into an authorized or unauthorized one, a new informational event for the unaudited observations will not be re-delivered. It is delivered only once for the observation bundle. However if one of the observations is manually set to unauthorized, then a violation is raised for the entire observation bundle.

When at least one observation in a bundle is in an unauthorized state, a violation is created. That violation becomes an event in the Incident Manager Console. Use the Incident Manager feature to set up a notification. For more information about this, on the Incident Manager page, click on the online help link, [Setting Up Notifications With Rules](#) under the [Setting Up Notifications](#) section under [Getting Started](#).

27.3.2.3 Notifying a User When an Authorized Observation Occurs

When an authorized observation occurs, it is not a typical for you to receive a notification on these observations since the activity that caused the observation was expected. If you are using change management reconciliation, you have an option to annotate the authorizing change request with the observation details. The updates to the change request is one way customers can learn of authorized activity. You can set filters in their change management system to let them know that a change request has had authorized activity against it.

27.4 Configuring Compliance Management

Before you can use the compliance features, compliance frameworks, compliance standards, and compliance standard rules must be defined for your enterprise.

The following sections describe how to define and maintain these compliance entities.

- [About Compliance Frameworks](#)
- [Operations on Compliance Frameworks](#)
- [About Compliance Standards](#)
- [Operations on Compliance Standards](#)
- [About Compliance Standard Rule Folders](#)
- [About Compliance Standard Rules](#)
- [Operations on Compliance Standards Rules](#)

27.4.1 About Compliance Frameworks

A compliance framework is a hierarchical structure where any node can be mapped to one or more compliance standards, compliance standard rule folders, and compliance standard rules. Compliance frameworks provide a way to map your standards to a structure similar to the regulatory or standards-based compliance structure you use in your company.

Managing Compliance Frameworks

To manage compliance frameworks, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click **Compliance Frameworks** tab.
3. Highlight the compliance framework you want to manage and choose the action you want to perform.

Frameworks Provided by Oracle and User-Defined Compliance Frameworks

There are compliance frameworks provided by Oracle and user-defined compliance frameworks.

- Compliance frameworks provided by Oracle
 - PCI DSS 2.0 (Payment Card Industry Data Security Standard) is a standard which you can use to evaluate your managed targets compliance with security and best practices standards.
 - Oracle Generic Compliance Framework is a standard set of compliance standards and associated controls for tracking changes and events taking place across your IT infrastructure for determining how well your organization is in compliance with your IT policies.

- User-defined compliance frameworks

You can define a compliance framework to satisfy the needs of your organization.

Compliance frameworks provided by Oracle cannot be deleted or edited. However, if you want to extend these frameworks, use the Create Like functionality to create your own user-defined frameworks based on the out-of-box frameworks and then edit the new frameworks.

Recommendation: It is highly recommended that you create a top level compliance framework like the ones provided for PCI and Oracle Generic compliance.

Example of Using the PCI Framework

If you follow the Payment Card Industry (PCI) framework, you may have a multiple level structure that mirrors the structure of PCI as follows:

- PCI DSS 2.0 - Payment Card Industry Data Security Standards compliance framework which contains:
 - Build and Maintain a Secure Network (PCI 2.0) compliance standard which contains:
 - * Encrypt all administrative access using SSH, VPN, or SSL/TLS (PCI 2.3) compliance standard rule

PCI is comprised of a series of Requirements in a hierarchy. There are 12 top-level requirements, each with smaller set of requirements. This hierarchy can be mirrored with a Compliance Framework.

A compliance framework (PCI 2.0, for example) contains a number of compliance standards that are specific to a target type. A single compliance score will be calculated for that compliance standard and then can be rolled up to all the compliance frameworks.

Benefits of Using Compliance Frameworks

Compliance standards are defined to perform tests on targets. Examples include: testing if a configuration value is set properly, test to see if real-time file changes are occurring, and so on. A compliance framework is a way to map how different control areas of your compliance initiative are going to be affected by the results of those tests.

An organization may choose to define a compliance framework that extends an out-of-box compliance framework. This is accomplished by creating a new compliance framework like the out-of-box compliance framework and include new or existing compliance standards. Then each compliance standard is mapped to an appropriate framework hierarchy folder so that any violation against the standard is also mapped to that framework folder. Each folder in the framework represents one control area.

Reasons for Using Compliance Frameworks

There are a number of reasons for creating compliance frameworks including:

- Mapping underlying IT violations to the regulatory and standard compliance controls used by your company so you can easily identify the compliance control areas that will be affected by the violations
- Compliance auditing at compliance specification level (for example, Payment Card Industry (PCI))
- Auditing, security evaluation, and trend analysis

What Compliance Frameworks Can Do

A compliance framework can:

- Represent industry-standard compliance control areas or can be created to match your internal frameworks in use.

Many companies may start by using an industry-standard framework, but modify it according to their own needs and auditing requirements. An organization may choose to create a new framework based on PCI, but add additional control areas that are not covered by PCI.

- Help in IT audits by identifying which compliance controls are at risk and may need compensating controls based on the violations. Without mapping your compliance checks to the control areas affected, it is hard to identify what the real impact would be in a compliance audit.

- Since compliance frameworks can contain compliance standards of different types (Repository, WebLogic Server Signature, Real-time monitoring), they provide a good way of grouping similar checks of different types for reporting purposes.

Usage Note

Evaluation Results for a repository rule may become invalidated if a compliance standard rule within a compliance framework is modified or deleted. Evaluation of a compliance standard always references the current compliance standard rule definition for each compliance standard rule within the compliance standard.

27.4.2 Operations on Compliance Frameworks

You can perform the following operations on a compliance framework:

- [Creating a Compliance Framework](#)
- [Creating Like a Compliance Framework](#)
- [Editing a Compliance Framework](#)
- [Deleting a Compliance Framework](#)
- [Exporting a Compliance Framework](#)
- [Importing a Compliance Framework](#)
- [Browsing Compliance Frameworks](#)
- [Searching Compliance Frameworks](#)

The following sections explain these operations.

Note: Before you perform any of the operations on compliance frameworks, ensure you have necessary privileges. For example, when creating a compliance framework, ensure you have access to the compliance standards you will be including during the definition of the framework. (See [Section 27.1.3.](#))

27.4.2.1 Creating a Compliance Framework

To make the creation for the compliance framework easier, ensure that the compliance standards, which will be referred to by the compliance framework, are already defined in the Cloud Control. You can add system out-of-the-box and user-defined compliance standards to any hierarchical element of the compliance framework. If you do not define the compliance standards before hand, you must add them later.

To create a compliance framework, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Frameworks** tab.
3. Click **Create** button.
4. Provide the Name and Author and click **OK**.
5. Once you have provided the information on the definition page, look at the options available when you right-click the name of the compliance framework (located at the top-left of the page). From this list you can create subgroups, include compliance standards, and so on.
6. Click **Save**.

Usage Notes

- Lifecycle status can be either Development or Production.

- Development

Indicates a compliance framework is under development and that work on its definition is still in progress. While in development mode, all management capabilities of compliance frameworks are supported including editing of the compliance framework and deleting the compliance framework. Results of development compliance standards will NOT be viewable in target and console home pages, and the compliance dashboard.

Lifecycle status default is Development. It can be promoted to Production only once. It cannot be changed from Production to Development.

- Production

Indicates a compliance framework has been approved and is of production quality. When a compliance framework is in production mode, its results are rolled up into a compliance dashboard, target and console home page.

Production compliance frameworks can only refer to Production compliance standards. A production compliance framework can be edited to add/delete references to production compliance standards ONLY!

Lifecycle status cannot be changed from Production to Development.

- All compliance frameworks with the same keyword will be grouped together when sorted by the Keyword column.
- If you modify a repository or WebLogic Server signature compliance standard that has been added to a compliance framework, either by editing the compliance standard directly, or by using Import to overwrite the compliance standard with new settings, the existing evaluations become invalid. That is, if this modified compliance standard was included in a compliance framework that was previously evaluated, and has evaluation results, these results are no longer viewable.

Adding a Compliance Standard to a Compliance Framework

Click on a framework folder element that you want to map a compliance standard to. Right click and select Add Standards to bring up a popup to allow you to select the standards to map to this folder.

Use the search criteria to minimize the number of compliance standards that display in the select list.

Once you make your selections, click **OK**. The framework hierarchy screen refreshes and shows your newly included compliance standards under the framework folder element.

Editing Importance

After you map the compliance standards that are to be part of the selected compliance framework folder, you can edit the importance of each compliance standard for this specific folder.

The importance impacts the way the compliance score is calculated for this compliance standard in this framework folder.

See Overview of Compliance Score and Importance for details on how this score is computed.

27.4.2.2 Creating Like a Compliance Framework

To create a compliance framework like another compliance framework, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Frameworks** tab.
3. On the Compliance Framework Library page, highlight the compliance framework you want to use as the base and click the **Create Like** button.
4. Customize the fields as needed.

Ensure that the Compliance Framework name is different from the original compliance framework and any other existing compliance frameworks.

5. Click **Save**.
6. You can then edit this newly created framework and add or remove standards, subfolders, or modify importance levels

27.4.2.3 Editing a Compliance Framework

Use the edit compliance framework feature to add new compliance standard rules to a compliance framework, or edit details of existing compliance frameworks, or remove compliance standards from the compliance framework.

To edit a compliance framework, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Frameworks** tab.
3. Highlight the compliance framework you want to edit and click the **Edit** button.
4. Update the properties as needed.

To add standards and subgroups, right-click the name of the framework located at the top left of the page.

5. Click **Save**.

Usage Notes

- Changing a compliance framework definition may impact trend analysis.
- The compliance standards you add to a compliance framework may be system-defined and user-defined compliance standards as displayed on the Compliance Standard Library page.
- If you modify a repository or WebLogic Server signature compliance standard that has been added to a compliance framework, either by editing the compliance standard directly, or by using Import to overwrite the compliance standard with new settings, the existing evaluations become invalid. That is, if this modified compliance standard was included in a compliance framework that was previously evaluated, and has evaluation results, these results are no longer viewable. The compliance framework evaluation results will again become visible after the next evaluation happens. The new evaluation includes the changes to the compliance standard within the compliance framework.
- The importance impacts the way the compliance score is calculated for this compliance standard in this framework folder.
- A compliance standard can be added to more than one compliance framework, and can have a different importance when added to a different compliance

framework. For example, you could have a compliance standard called Check Password Expired which flags user accounts with expired passwords. This compliance standard may be a member of two compliance frameworks: All System Passwords Secure and 30-day Password Validation. The All System Passwords compliance framework verifies a password's security, whereas the 30-day Password Validation compliance framework checks the date that this password was last set.

- The Check Password Expired compliance standard could have Extremely High importance for the 30-day Password Validation compliance framework, since this check is warning users that their passwords are about to expire.
- In the All System Passwords Secure compliance framework, the Check Password Expired compliance standard could have a Normal importance, and other added compliance standards that do security checks could have a higher importance within the compliance framework.

27.4.2.4 Deleting a Compliance Framework

To delete a compliance framework, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Frameworks** tab.
3. Highlight the compliance framework you want to delete, click **Delete** button.
4. Confirm that you want to delete the compliance framework by clicking **OK**.

Usage Notes

- You can delete a single compliance framework or a list of compliance frameworks. When you delete a compliance framework, the associated metadata and evaluation results are also deleted.
- **YOU CANNOT DELETE COMPLIANCE FRAMEWORKS DEFINED BY ORACLE.** These are indicated by the presence of a lock icon in front of the compliance framework name on the compliance framework listing page.

27.4.2.5 Exporting a Compliance Framework

The Export feature provides a mechanism for transporting user-defined compliance framework definitions across Management Repositories and Cloud Control instances. The export stores the definitions in an operating system file. Because the exported compliance framework definitions are in XML format, they conform to the Oracle Compliance Standard Definition (XSD) format. You can then change the definition of the compliance framework and re-import the generated compliance framework definitions into another Management Repository.

To export a compliance framework, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Frameworks** tab.
3. Highlight the compliance framework you want to export.
4. From the **Actions** menu, select **Export**.
5. Provide the file name to which the compliance framework definition is to be exported. Determine whether is to be a shallow or deep export. In a shallow export, no leaf level rules or compliance standards are to be exported. In a deep export, all leaf level rules and compliance standards are exported.

The system generates an XML representation of the compliance framework in the directory and file you specify.

27.4.2.6 Importing a Compliance Framework

Importing allows you to re-use a compliance framework that you already have, share framework definitions across multiple instances of Cloud Control, or enable offline editing of the framework.

Before you import a compliance framework, ensure the compliance framework to be imported is defined in a file. The file should be locally accessible to the browser you are using to access Cloud Control. Also ensure that you have privileges to access the compliance framework definition XML file to be imported.

To import a compliance framework, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Frameworks** tab.
3. From **Actions** menu, select **Import**.
4. Provide the file name from which the compliance framework definition (as per Compliance Framework XSD) will be imported. Specify whether to override an existing definition if one already exists. Specify whether to import referring content as well, that is, shallow or deep import. In a shallow import, no leaf level rules or compliance standards are to be imported. In a deep import, all leaf level rules and compliance standards are imported. In a deep import, real-time monitoring facets are also imported for real-time monitoring type of rules.
5. Click **OK**.

27.4.2.7 Browsing Compliance Frameworks

To browse a compliance framework, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Frameworks** tab.
3. To view the details of a particular compliance framework, highlight the compliance framework and click **Show Details**.

27.4.2.8 Searching Compliance Frameworks

To search for a compliance framework, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Frameworks** tab.
3. In the Search portion of the page, provide criteria to use to narrow the search.
4. Click **Search**.

27.4.2.9 Browsing Compliance Framework Evaluation Results

To browse compliance framework evaluation results, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. Click the **Compliance Frameworks** tab and then the **Evaluation Results** tab.
3. Highlight the compliance framework and click **Show Details** to view the details of a particular compliance framework.

Results include the following:

- Average compliance score for different targets evaluated for compliance standards referred to by the compliance framework
- Count of target evaluations (critical, warning, compliant) for different compliance standards referred to by the compliance framework
- Count of violations (critical, warning, minor warning) related to compliance standards referred to by the compliance framework

27.4.2.10 Searching Compliance Framework Evaluation Results

To search compliance framework evaluation results, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. Click the **Compliance Frameworks** tab and then the **Evaluation Results** tab.
3. In the Search portion of the page, provide criteria to use to narrow the search.
4. Click **Search**.

27.4.2.11 Browsing Compliance Framework Errors

To browse compliance framework errors, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. Click the **Compliance Frameworks** tab and then the **Errors** tab.

Usage Notes

The error may be an unexpected internal error or an error in the test.

Evaluation errors can often be due to configuration and installation issues. See the following manuals for information:

- *Oracle Enterprise Manager Cloud Control Basic Installation Guide*
- *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*

If the installation and configuration are correct and the errors persist, call Oracle for assistance.

27.4.2.12 Searching Compliance Framework Errors

To search for compliance framework errors, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. Click the **Compliance Frameworks** tab and then the **Errors** tab.
3. In the Search portion of the page, provide criteria to use to narrow the search.
4. Click **Search**.

Usage Notes

The error may be an unexpected internal error or an error in the test.

Evaluation errors can often be due to configuration and installation issues. See the following manuals for information:

- *Oracle Enterprise Manager Cloud Control Basic Installation Guide*

- *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*

If the installation and configuration are correct and the errors persist, call Oracle for assistance.

27.4.2.13 Verifying Database Targets Are Compliant with Compliance Frameworks

For auditors to verify that database targets are in compliance with the compliance frameworks, the Cloud Control structure needs to be defined. The steps to provide this structure include the following:

1. Super Administrator creates three Cloud Control users: Compliance Author, IT Administrator, and Compliance Auditor.
2. Super Administrator assigns the appropriate roles and privileges to the Compliance Author and IT Administrator.
3. Super Administrator assigns the same target privileges to IT Administrator and Compliance Auditor.
4. Compliance Author logs in to Cloud Control and views out-of-box compliance frameworks, compliance standards, and compliance standard rules.
He then enables and disables the appropriate compliance standard rules and creates new compliance standard rules.
5. IT Administrator logs in to Cloud Control and associates the targets for which he has target privileges with the appropriate compliance standards.
6. IT Administrator sets up the correct configuration parameters and settings for the compliance frameworks, compliance standards, and compliance standard rules for a particular target.
He then creates a monitoring template from this target and applies it to the other targets, to which he has privileges, that require compliance standards.
7. Compliance Auditor logs in to Cloud Control to view the violations and errors at the Enterprise level, for which he has view privileges, and at each target level.
He would then take the necessary actions to rectify the errors and violations.

27.4.3 About Compliance Standards

A compliance standard is a collection of checks or rules. It is the Cloud Control representation of a compliance control that must be tested against some set of IT infrastructure to determine if the control is being followed.

Compliance standards are made up of the following in a hierarchical structure (see [Figure 27-9](#)):

- Compliance standard rules
- Rule folders that can include nested rule folders and individual compliance standard rules.

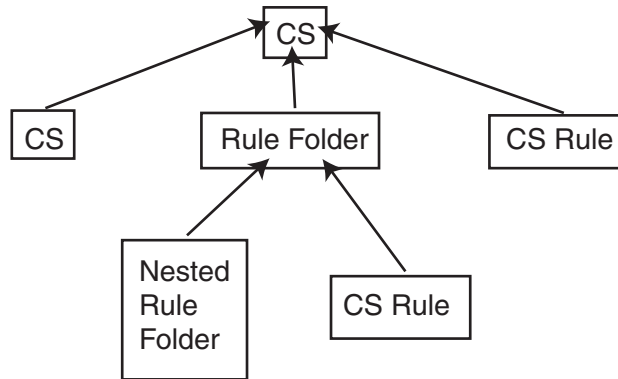
Rule Folders are hierarchical structures that contain compliance standard rules. A rule folder has an importance attribute that denotes the importance of the rule folder relative to its siblings at the same level. This importance is considered when determining compliance scores being rolled up from other sibling rule folders. A certain rule folder may have multiple tests that occur, in this way a certain test can be given more weight than other tests.

- Included compliance standards. A compliance standard can include other compliance standards.

Figure 27–9 Compliance Standard Definition

Key:

CS - compliance standard



What Compliance Standards Can Do

- Can represent industry-wide standards. A compliance standard is applicable to a single target type.
- Be used as a reference configuration or a certified configuration
- Be a collection of compliance standard rules describing best practices in an enterprise

For example, when a target fails to adhere to a compliance standard, the target is not in compliance with the compliance standard.

Accessing Compliance Standards

The compliance standards, including those provided by Oracle, are available on the Compliance Standard Library page. To access this page, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standards** tab.

To view the compliance standard rules associated with the compliance standard, click the name of the compliance standard and click **Show Details**. Once the Compliance Standard Detail page appears, right click the name of the standard located at the top left of the page, and select either **Expand** or **Expand All Below**.

Note: The compliance standards defined by Oracle cannot be changed. However, you can create a standard similar to the one provided by Oracle by using the Create Like feature.

General Usage Notes for Compliance Standards

You can override an existing compliance standard by checking the **Overwrite existing compliance standards** check box. As a result, evaluations of compliance standards require that the compliance standard is associated to one or more targets.

- For repository compliance standards, evaluation starts after the standard is associated with a target based on data collected from that target in the Management Repository.

- For WebLogic Server compliance standards, evaluation happens when the Management Agent-side evaluation metric is refreshed. The refresh occurs once every 24 hours for Oracle WebLogic Domain, Oracle WebLogic Java EE Server, and Oracle WebLogic Cluster targets.
- For Real-time Monitoring compliance standards, monitoring at the Management Agent starts when a compliance standard is associated to a target. A violation occurs when an observation bundle contains at least one observation that is unauthorized

Usage Note Specific to Repository Rules

If you manually type a WHERE clause in the compliance standard rule XML definition, then the < (less than) symbol must be expressed as <, to create a valid XML document. For example:

```
<WhereClause>:status &lt; 100</WhereClause>
```

Example of How to Set Up Compliance Standards for Auditing Use

For auditors to verify that database targets are in compliance with the compliance frameworks, the Cloud Control structure needs to be defined. The steps to provide this structure includes the following:

1. Super Administrator creates three Cloud Control users: Compliance Author, IT Administrator, and Compliance Auditor.
2. Super Administrator assigns the appropriate roles and privileges to the Compliance Author and IT Administrator.
3. Super Administrator assigns the same target privileges to IT Administrator and Compliance Auditor.
4. Compliance Author logs in to Cloud Control and views out-of-box compliance frameworks, compliance standards, and compliance standard rules.
He then enables and disables the appropriate compliance standard rules and creates new compliance standard rules.
5. IT Administrator logs in to Cloud Control and associates the targets for which he has target privileges with the appropriate compliance standards.
6. IT Administrator sets up the correct configuration parameters and settings for the compliance frameworks, compliance standards, and compliance standard rules for a particular target.
He then creates a monitoring template from this target and applies it to the other targets, to which he has privileges, that require compliance standards.
7. Compliance Auditor logs in to Cloud Control to view the compliance dashboard, violations and errors at the Enterprise level, for which he has view privileges, and at each target level.

He would then take the necessary actions to rectify the errors and violations.

27.4.4 Operations on Compliance Standards

You can perform the following operations on a compliance standard:

- [Creating a Compliance Standard](#)
- [Creating Like a Compliance Standard](#)
- [Editing a Compliance Standard](#)

- [Deleting a Compliance Standard](#)
- [Exporting a Compliance Standard](#)
- [Importing a Compliance Standard](#)
- [Browsing Compliance Standards](#)
- [Searching Compliance Standards](#)

The following sections explain these operations.

Note: Before you perform any of the operations on compliance standards, ensure you have necessary privileges. For example, when creating a compliance standard, ensure you have access to the compliance standard rules you will be including during the definition of the compliance standard. (See [Section 27.1.3](#).)

27.4.4.1 Creating a Compliance Standard

You can use the compliance standards provided by Oracle, for example, Security Configuration for Oracle Database, or create your own standard.

Before creating a compliance standard, ensure the compliance standards and compliance standard rules, which will be referred to by the compliance standard, are defined in the Management Repository.

To create a compliance standard, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standards** tab.
3. Click the **Create** button. You will be prompted for the Name, Author, target type to which the standard is applicable, and the type of compliance standard (Repository, WebLogic Server Signature, Real-time Monitoring). Click **OK**.
4. On the resulting Compliance Standard Detail page, provide the property values. Click **Add** to either add a keyword by which this standard is identified or use an existing keyword.
5. To further define the compliance standard, right-click the name of the compliance standard located at the top left of the page. From this menu, you can create rule folders, add rules, and include compliance standards.

By using rule folders, you can view the summary of results, categorized by the targets that were evaluated against the selected rule folder and the Compliance Standard Rules evaluated for the selected rule folder.

6. Click **Save**.

Once you define the compliance standard, associate the standard with a target and define the target type-specific settings.

1. While on the Compliance Standards Library page, ensure the correct compliance standard is highlighted.
2. Click the **Associate Target** button.
3. On the **Target Association for Compliance Standard** page, click **Add** to choose the target to be evaluated against the standard.
4. In the **Search and Select: Targets** popup, choose the appropriate targets.
5. Click **Select**.

After you associate the targets with the compliance standard, you can edit the parameters associated with the target.

1. While on the **Target Association for Compliance Standard** page, click **Edit**.
2. On the **Customize Compliance Standard Parameters** page, change the parameters as needed.

Note: You can also associate a compliance standard with a target from the target home page. At the top left of the target's home page, right click the name of the target. On the resulting menu, select **Compliance**, then select **Standard Associations**.

Including a Compliance Standard into Another Compliance Standard

Use the Include Compliance Standard page to select one or more compliance standards to be included into the compliance standard. This list is prefiltered by the target type of the compliance standard.

To include a compliance standard into another compliance standard:

1. From the Compliance Standard Library page, highlight the compliance standard to which you want to add another compliance standard.
2. Click the **Edit** button.
3. On the Properties page, right-click the node, located at the top left of the page.
4. On the resulting menu, select **Add Standards**.
5. Select the compliance standard to include. Click **OK**.

When you include a compliance standard within another top level compliance standard, the included standard must be of the same target type as the top level compliance standard. For composite target types, one of the member target types of the composite target type of the top level standard is a member target type within the top level composite target type.

Note that a root compliance standard is associated to a root target (of composite target type). Compliance standards are associated to member targets of the same applicable target type and target filter criteria.

6. On the **Properties** page, choose the **Importance** for the compliance standard you just included. Click **Save**.
7. After the compliance standard is included, highlight the root compliance standard. The Properties page displays a set of parameters.

A parameter is a variable that can be used by one or more compliance standard rules contained in that compliance standard. When a compliance standard rule references a parameter, the parameter's actual value is substituted at compliance standard rule evaluation time. It is through the use of parameters that customizations of compliance standards is supported.

Usage Notes

- Because compliance standards are hierarchical, the top node in the tree is known as the root node.
- When you create a compliance standard, the version is 1.
- Lifecycle status default is Development. It can be promoted to Production only once. It cannot be changed from Production to Development.

- Development

Indicates a compliance standard is under development and that work on its definition is still in progress. While in Development mode, all management capabilities of compliance standards are supported including complete editing of the compliance standard, deleting the compliance standard, and so on. However, while the compliance standard is in Development mode, its results are not viewable in Compliance Results nor on the target or Cloud Control home page.

- Production

Indicates a compliance standard has been approved and is of production quality. When a compliance standard is in production mode, you have limited editing capabilities, that is, you can add references to production rules, and you can delete references to rules ONLY from a compliance standard. All other management capabilities such as viewing the compliance standard and deleting the compliance standard will be supported. Results of production compliance standards are viewable in target and console home pages, and the compliance dashboard. Production compliance standards can only refer to production compliance standards and production compliance standard rules.

Once the mode is changed to Production, then its results are rolled up into compliance dashboard, target home page, and Cloud Control home page. Production compliance standards can only refer to other production compliance standards and production compliance standard rules. A production compliance standard can be edited to add and delete references to production compliance standards and production compliance standard rules ONLY.

27.4.4.2 Creating Like a Compliance Standard

To create a compliance standard like another compliance standard, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standards** tab.
3. Click the **Create Like** button.
4. Customize the fields as needed.

The name has to be different than an existing Compliance Standard.

5. Click **Save**.

27.4.4.3 Editing a Compliance Standard

You can customize compliance standards by editing the existing compliance standard rule settings. You can change the added rules' importance for the compliance score calculation, prevent template override, override default parameter values (when possible), and exclude objects from a compliance standard rule's evaluation (when possible).

Note: You cannot edit an out-of-box compliance standard, that is, a compliance standard defined by Oracle.

To edit a compliance standard, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standards** tab.
3. Highlight the standard you want to edit and click the **Edit** button.

4. Update the parameters as needed.
5. Click **Save**.

27.4.4.4 Deleting a Compliance Standard

Before you delete a compliance standard, ensure the compliance standard is not in use by a compliance framework. You must remove any references to the compliance standard in all compliance frameworks.

Note: You cannot delete an out-of-box compliance standard, that is, a compliance standard provided by Oracle.

To delete a compliance standard, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standards** tab.
3. Highlight the compliance standard you want to delete, click **Delete** button.
4. Confirm that you want to delete the standard by clicking **OK**.

27.4.4.5 Exporting a Compliance Standard

The Export feature provides a mechanism for transporting user-defined compliance standard definitions across Management Repositories and Cloud Control instances. The export stores the definitions in an operating system file. Because the exported compliance standard definitions are in XML format, they conform to the Oracle Compliance Standard Definition (XSD) format. You can then change the definition of the compliance standard and re-import the generated compliance standard definitions into another Management Repository.

Before you export a compliance standard, ensure that you have privileges to access the compliance standard to be exported.

To export a compliance standard, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standards** tab.
3. Highlight the standard you want to export.
4. From the **Actions** menu, select **Export**.
5. Provide the file name to which the standard definition is to be exported. Determine whether is to be a shallow or deep export. In a shallow export, no leaf level rules or compliance standards are to be exported. In a deep export, all leaf level rules and compliance standards are exported.
6. The XML representation of the compliance standard is generated. The file is located in the directory you specify.

27.4.4.6 Importing a Compliance Standard

The Import feature uploads an XML-based compliance standard definition file containing definitions of a single user-defined compliance standard or a list of user-defined compliance standards. This upload creates a new user-defined compliance standard or a list of user-defined compliance standards. This compliance standard must have been previously exported.

The compliance standard xml definition must comply with the compliance standard XML Schema Definition (XSD) as defined in User-Defined Compliance Standard XML Schema Definition.

Before importing a compliance standard, ensure the compliance standard to be imported is defined in a file. The file should be locally accessible to the browser you are using to access Cloud Control. Also ensure that you have privileges to access the compliance standard definition XML file to be imported.

To import a compliance standard, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standards** tab.
3. From the **Actions** menu, select **Import**.
4. Provide the file name from which the compliance framework definition (as per Compliance Framework XSD) will be imported. Specify whether to override an existing definition if one already exists. Specify whether to import referring content as well, that is, shallow or deep import.
5. Click **OK**.

You can override an existing compliance standard by checking the **Overwrite existing compliance standards** check box. As a result:

- If you override a compliance standard, the override deletes all target and template associations, as well as evaluation results for that compliance standard.
- If the overwritten compliance standard is part of a compliance framework, the compliance standard is updated in the compliance framework. However, the evaluation results for that compliance standard within the compliance framework are invalidated.

27.4.4.7 Browsing Compliance Standards

To browse a compliance standard, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standards** tab.
3. To view the details of a particular standard, highlight the standard and click **Show Details**.

27.4.4.8 Searching Compliance Standards

To search for compliance standards, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standards** tab.
3. In the Search portion of the page, provide criteria to use to narrow the search.
4. Click **Search**.

27.4.4.9 Browsing Compliance Standard Evaluation Results

To browse compliance standard evaluation results, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. Click the **Compliance Standards** tab and then the **Evaluation Results** tab.
3. Highlight the compliance standard and click **Show Details** to view the details of a particular standard.

Results include the following:

- Average compliance score for different targets
- Count of target evaluations (critical, warning, compliant)
- Count of violations (critical, warning, minor warning)

27.4.4.10 Searching Compliance Standard Evaluation Results

To search for compliance standard evaluation results, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. Click the **Compliance Standards** tab and then the **Evaluation Results** tab.
3. In the Search portion of the page, provide criteria to use to narrow the search.
4. Click **Search**.

27.4.4.11 Browsing Compliance Standard Errors

To browse compliance standard evaluation errors, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. Click the **Compliance Standards** tab and then the **Errors** tab.

27.4.4.12 Searching Compliance Standard Errors

To search for compliance standard errors, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Results**.
2. Click the **Compliance Standards** tab and then the **Errors** tab.
3. In the Search portion of the page, provide criteria to use to narrow the search.
4. Click **Search**.

Usage Notes

- Use the Evaluation Errors page to view the errors that occurred as a result of metric collection, as well as those that occurred during the last evaluation.
- Use the search filter to view only those evaluation errors that meet a set of search criteria that you specify.
- Click the message in the Message column to decide what your course of action should be to resolve the error.
- On initial display, the Evaluation Errors page shows all the evaluation errors.
- Normally the results of an evaluation overwrite the previous evaluation's results. However, in the case of evaluation failure or data provider collection failure, the previous results are left untouched.

Once the underlying problem is fixed, the error is no longer reported.

Example of Search Filter

By default, all the evaluation errors in your enterprise configuration appear in the results table. However, you can specify a set of search criteria and then perform a search that will display only the evaluation errors that meet those criteria in the results table.

For example, if you choose Host in the Target Type list, contains in the Target Name list, and "-sun" in the adjacent Target Name text field, and then click **Go**, Cloud

Control displays, in the results table, only the compliance standard rule evaluation errors for the hosts that contain "-sun" in their names.

27.4.4.13 Associating a Compliance Standard with Targets

After you create a compliance standard, you can associate the standard with one or more targets. As part of the association, you can customize parameters, that is, the importance of the standard in relation to the target, status of the compliance standard evaluation, reason for changing the evaluation status, and the thresholds.

Before you associate a compliance standard with a target, ensure you have privileges to access the targets you want to associate compliance standards to.

To associate a compliance standard with a target, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standards** tab.
3. Highlight the compliance standard you want to associate with various targets. Click the **Associate Target** button.
4. Select the targets you want to associate with this compliance standard. Click **OK**.
5. With the compliance standard still highlighted, click the **Override Target Type Settings** button.
6. Customize the critical and warning thresholds and importance as needed.

By changing critical and warning thresholds, you signify how the Compliance standard score event is generated. For example, if the actual score is less than the critical threshold, then a critical score event is raised.

Changing the importance can change the compliance score. The importance denotes how important the compliance standard is in the hierarchy.

7. Click **OK**.

To further customize the evaluation of a compliance standard against a target, you can alter compliance standard parameters: importance, critical threshold, and warning threshold. Customizations can also be made on the compliance standard rules used within the compliance standards. For example, for the Secure Ports compliance standard rule, `DFLT_PORT` is an override parameter. You can change the default value of the port. You can also exclude objects from the evaluation, for example a particular port from the evaluation.

Note: For real-time monitoring, you can change parameters that are used in facet patterns. You can also change Automatic Change Management reconciliation settings.

By changing critical and warning thresholds, you signify how the Compliance standard score event is generated. For example, if the actual score is less than the critical threshold, then a critical score event is raised.

Best Practices

You can perform compliance association in two ways: for testing and editing, and production and mass associations.

- For testing and editing a standard/target and standard rule, or rule folder/target association settings purposes, associate the target with a compliance standard as previously described in this section.

Using the Compliance UI, you can:

- Test the association and remove it after testing is complete.

- Edit the association for importance, evaluation status, and thresholds.

Note: You *cannot* edit an association using the Administration Groups and Template Collections page.

- For production and mass associations, associate the target using the Administration Groups and Template Collections page:

From the **Setup** menu, select **Add Target**, then select **Administration Groups**. Click the **Associations** tab.

Because each Administration Group in the hierarchy is defined by membership criteria, a target is added to the group only if it meets the group's membership criteria. Therefore, when a target is successfully added to a group, it is automatically associated with the eligible compliance standards for that group. This makes it easier to associate a target to a large number of compliance standards.

27.4.4.14 Viewing Real-time Monitoring Compliance Standard Warnings

When you associate a real-time monitoring compliance standard to targets, there is a chance that there are setup steps that were not followed on the target to enable real-time monitoring or there could be inconsistency with the configuration. Any warnings will be shown on the Associate Targets screen. This screen is reached by selecting a compliance standard and selecting **Associate Targets** button. If there are any warnings, there will be a warning icon with a link above the table of target associations. Clicking on this link will take you to a screen that lists all current warnings for this compliance standard.

All warnings can be fixed by correcting some configuration problem on the host/target you are monitoring or by fixing rule/facet content. Once the underlying problem is fixed, these warnings will be cleared automatically.

This list of warnings is also available on the Real-time Observations page (from the Enterprise menu, select **Compliance**, then select **Real-time Observations**) where you can pick one of three types of reports to view your observations. The bottom half of the screen shows all active warnings across all targets and compliance standards related to real-time monitoring.

27.4.4.15 Enabling Security Metrics

Because security collections are disabled out-of-box, they must be enabled before using security features like security compliance standards, reports, and so on.

To enable Security metrics, follow these steps:

1. From the **Enterprise** menu, select **Monitoring**, then select **Monitoring Templates**.
2. In the Search area, select **Display Oracle provided templates and Oracle Certified templates** and click **Go**.
3. Select **Oracle Certified-Enable Database Security Configuration Metrics** and click **Apply**.
4. In the Destination Targets region on the Apply Monitoring Template Oracle Certified-Enable Database Security Configuration Metrics: General page, click **Add**.
5. On the Search and Select: Targets page, select the database instances in which you are interested and click **Select**.

6. In the Destination Targets region of the Apply Monitoring Template Oracle Certified-Enable Database Security Configuration Metrics: General page, select the database instances in which you are interested and click OK.

After you click OK, a confirmation message on the Monitoring Templates page appears.

27.4.4.16 Considerations When Creating Compliance Standards

A compliance standard will refer to one or more Compliance Standard Rules. When creating a compliance standard, the standard should be granular enough that it can be appropriately mapping to one or more related Compliance Frameworks. For example, consider this Compliance Framework structure that exists in Cloud Control based on PCI:

- PCI - Payment Card Industry Compliance Framework
 - PCI Requirement 10 - Regularly monitor and test networks
 - * PCI 10.5 - Secure audit trails

Many compliance standards will exist that should mapped to this part of the Compliance Framework structure, each with their own rules to address this specific requirement. One may check that audit settings are set properly. Another may be used to check in real-time if anyone changes an auditing configuration. Another standard may check that regular users are not trying to read from an audit trail.

In this example, the "audit trail" referenced in the Compliance Framework can relate to many different types of targets. Oracle Database, WebLogic, Cloud Control, EBS, and Peoplesoft all have their own types of audit trails that all need to be secured. Any Standards created to monitor these target-specific audit trails would map to the same Compliance Framework named "PCI 10.5 - Secure Audit Trails."

If compliance standards are structured in a granular way so that they can map to existing and future compliance frameworks, then violations in a rule can be rolled up to impact the score of the compliance framework properly.

27.4.5 About Compliance Standard Rule Folders

Rule Folders are optional hierarchical structures used to group similar compliance standard rules within a compliance standard. You can add individual compliance standard rules to a compliance standard, or group them if you have a large number of rules in a standard. A compliance standard rule can be added to multiple Rule Folders within a compliance standard, each with different importance settings. Rule Folders can be nested within a compliance standard.

A rule folder has an importance attribute that denotes the importance of the rule folder relative to its siblings at the same level. This importance is considered when determining compliance scores being rolled up from other sibling rule folders. A certain rule folder may have multiple tests that occur, in this way a certain test can be given more weight than other tests.

The following topics address compliance standard rule folders:

- [Creating Rule Folders](#)
- [Managing Rule Folders in a Compliance Standard](#)

27.4.5.1 Creating Rule Folders

To create a rule folder, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standards** tab.
3. On the Compliance Standard Library page, highlight the compliance standard and click **Edit**.
4. On the **Properties** page, right-click the name of the compliance standard. The name of the standard is located in the top-left corner of the page.
5. Select **Create Rule Folder**.
6. Type the name of the folder and click **OK**.
7. On the **Properties** page, provide a description, ReferenceUrl, and importance. See [Section 27.2.8](#) for additional information regarding importance.

27.4.5.2 Managing Rule Folders in a Compliance Standard

After you create a rule folder and populate it with compliance standard rules, you can perform the following actions on the folder:

- Edit the tree structure by re-ordering the Rule Folder, Rule Reference, and Compliance Standard Reference nodes in the tree or by deleting any of these nodes.
- Select any node (except the top-level Compliance Standard node) object and then click **Remove** menu item from context menu. The Remove option is disabled on the root node. You can also select multiple objects and click **Remove** to delete multiple nodes.

27.4.6 About Compliance Standard Rules

A compliance standard rule is a test to determine if a configuration data change affects compliance. Based on the result of the test, a compliance score is calculated. These rule compliance scores are rolled up to compute the compliance standard score and then this score can be rolled up and reported along with the compliance framework scores.

Types of Compliance Standard Rules

There are three types of compliance standard rules are:

- **Repository Rules**
Used to perform a check against any metric collection data in the Management Repository.
Used for checking the configuration state of one or multiple targets. A rule is said to be compliant if it is determined that the configuration items do in fact meet the desired state and the rule test failed to identify any violations. Otherwise, a rule is said to be non-compliant if it has one or more violations. The data source that is evaluated by a compliance standard rules test condition can be based on a query against the Cloud Control Management Repository. A compliance standard rules test condition can be implemented using a threshold condition based on the underlying metrics (or queries) column value or SQL expression or a PLSQL function. To use a rule, it must be associated to one or more compliance standards. The compliance standard then will be associated to one or more targets. This effectively enables this rule to be evaluated against these targets.
- **WebLogic Server Signature Rules**
WebLogic Server signature rules describe potential problems based on information about WebLogic Servers and the environment in which they are

deployed, including Java Virtual Machines (JVMs), operating systems, and databases. Signature rules contain executable logic that can identify specific versions of these products, as well as their configuration settings.

- **Real-time Monitoring Rules**

Real-time monitoring rules monitor actions that users perform on targets. The types of actions that can be monitored include file changes, process starts and stops, user login/logouts, and database changes. These actions may lead to configuration changes and compliance risks. The actions are detected in real-time as observations at the time the action occurs enabling capture of the user, process, and exact time of the action.

27.4.7 Operations on Compliance Standards Rules

The following sections explain the operations you can perform on compliance standard rules.

- [Creating a Repository Compliance Standard Rule](#)
- [Creating a WebLogic Server Signature Compliance Standard Rule](#)
- [Creating a Real-time Monitoring Compliance Standard Rule](#)
- [Creating Like a Compliance Standard Rule](#)
- [Editing a Compliance Standard Rule](#)
- [Deleting a Compliance Standard Rule](#)
- [Exporting a Compliance Standard Rule](#)
- [Importing a Compliance Standard Rule](#)
- [Browsing Compliance Standard Rules](#)
- [Searching Compliance Standard Rules](#)

Note: Before you perform any of the operations on compliance standard rules, ensure you have the necessary privileges. (See [Section 27.1.3, "Privileges and Roles Needed to Use the Compliance Features"](#).)

27.4.7.1 Creating a Repository Compliance Standard Rule

To create a repository compliance standard rule to check if a target has the desired configuration state based on collected configuration data, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standard Rules** tab.
3. Click the **Create** button.
4. In the Create Rule popup, select Repository Rule as the type.
5. Click **OK**.
6. On the next screen, you are asked to fill out several key attributes of the rule:
 - **Rule Name**
Provide a unique name for the rule.
 - **Rule Lifecycle State**
Set whether the state of this rule is development or production. Development means that the rule is still being defined or tuned and is not yet ready to be

used on targets yet. After you promote a rule to production, you cannot change it back to development.

- **Severity**

The rule can have a severity level, which could be Critical (serious issue if this rule is violated), Warning (not a serious issue if violated), or Minor Warning (a minor issue if violated). Severity impacts the compliance score along with the importance that may be set for this rule when it is added to a compliance standard.
- **Applicable To**

Target type this rule works against.
- **Target Property Filter**

You can specify specific target properties that determine which targets this rule can work against when it is associated with a compliance standard. These properties are Operating System, Target Lifecycle State, Target Version, and Target Platform. When you specify a target property filter for this rule, for instance for Linux OS, it will only be applicable to targets on Linux Operating System.
- **Description**

Description of the rule
- **Rationale**

Text describing what this rule is checking and what the effect of a violation of this rule may be.
- **Recommendation**

Recommendation text describing how to fix a problem when a violation occurs.
- **Reference URL**

URL to a document that describes the compliance control in more details. Many times these documents may be stored in a content management system.
- **Keywords**

Keywords can be assigned to a rule so that you can control how data is organized in various reports.

7. Click **Next**.
8. On the next screen, you need to provide a SQL query that will execute against the Cloud Control Management Repository. You can directly enter the SQL query, or click the Model Query button to enter a screen that will guide you through choosing the query content.
9. Enter Compliant and Non-Compliant Message. These are the messages that will be shown in regards to the evaluation. When a violation occurs, the Non-Compliant message will be the string describing the event under the Incident Management capabilities.
10. Click **Next**.
11. On the next screen, you will see the columns that will be returned from this query as part of the evaluation results. You can modify the display name of each column as needed.

12. On this screen, you also need to set the condition you are checking against the returned query results to look for a violation. Your condition check can be a simple one based on the column name and a comparison operator of the value. Or you can compose a SQL condition by providing parameter names and providing a where clause to add to the evaluation query.
13. If you are using the SQL condition, you can click the **Validate Where Clause** button to check for any issues with your condition
14. Click **Next**.
15. The next screen will allow you to test your rule. You can choose a target in your environment and click the Run Test button. Any issues with the rule will be displayed and you can resolve them before saving the rule.
16. Click **Next**.
17. The final page allows you to review everything you have configured for this rule. Ensure that everything is correct and click the Finish button to save the rule.

Additional Notes for Repository Rules

- All rules are visible in the global rule library and are visible to all users.
- Once the compliance standard rule is created, it is not automatically evaluated. Users must associate a rule to a compliance standard before it can be used. Only when a compliance standard is associated with one or more targets will a rule evaluation occur. Rules cannot be evaluated directly.
- One rule can be associated to multiple compliance standards.
- Various attributes of a rule can be customized through the compliance standard this rule is associated with. These customizations occur in the Compliance Standard screens. One of these attributes that can be customized per compliance standard is the importance of the rule in relationship to this standard.
- Because the user-defined compliance standard rule is defined by a privileged user, only privileged users can modify the compliance standard rule. Violation results are available to all users.
- To share this user-defined compliance standard rule with other privileged users, provide the XML schema definition (using the Export feature) so they can import the compliance standard rule to their Management Repository.
- You can minimize scrolling when reading the Description, Impact, and Recommendation information by restricting the text to 50 characters per line. If more than 50 characters are needed, start a new line to continue the text.
- Look at the context-sensitive help for information for each page in the Compliance Standard Rule wizard for specific instructions.
- If you manually type a WHERE clause in the compliance standard rule XML definition, then the < (less than) symbol must be expressed as <, to create a valid XML document. For example:

```
<WhereClause>:status &lt; 100</WhereClause>
```

27.4.7.2 Creating a WebLogic Server Signature Compliance Standard Rule

There are several hundred out-of-the box WebLogic Server signature rules designed to uncover compliance violations known to occur in WebLogic installations based primarily on in-depth knowledge of common pitfalls and best practices. You can also create your own rules to extend the checks that are performed.

A signature describes a potential problem in a WebLogic installation. It consists of categorization metadata, a user-readable description of the problem, and an XQuery expression for evaluating whether the problem exists at the target.

A WLS Signature rule is an Management Agent-side rule that checks a signature definition against an associated target for the existence of the problem the signature defines. WebLogic Server targets include: WLS Domain; WLS Cluster; WebLogic Managed Server. The first two are composite target types: logical groupings of instances of simple WebLogic Server targets. Rules must be evaluated against the whole domain or cluster to render meaningful violation results.

WLS Signature rules, like other compliance rules, are grouped into Compliance Standards, which are logical groupings based on signature metadata such as severity and remedy.

To create a WebLogic Server Signature compliance standard rule to evaluate if certain configuration settings satisfy known good configurations, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standard Rules** tab.
3. Click the **Create** button.
4. In the Create Rule popup, select the WebLogic Server Signature rule type.
5. Click **OK**.
6. On the next screen, you are asked to fill out several key attributes of the rule:
 - **Rule Name**
Provide a unique name for the rule.
 - **Rule Lifecycle State**
Set whether the state of this rule is development or production. Development means that the rule is still being defined or tuned and is not yet ready to be used on targets yet. After you promote a rule to production, you cannot change it back to development.
 - **Severity**
The rule can have a severity level, which could be Critical (serious issue if this rule is violated), Warning (not a serious issue if violated), or Minor Warning (a minor issue if violated). Severity impacts the compliance score along with the importance that may be set for this rule when it is added to a compliance standard.
 - **Applicable To**
Target type this rule works against.
 - **Target Property Filter**
You can specify specific target properties that determine which targets this rule can work against when it is associated with a compliance standard. These properties are Operating System, Target Lifecycle State, Target Version, and Target Platform. When you specify a target property filter for this rule, for instance for Linux OS, it will only be applicable to targets on Linux Operating System.
 - **Description**
Description of the rule

- Rationale

Text describing what this rule is checking and what the effect of a violation of this rule may be.
 - Recommendation

Recommendation text describing how to fix a problem when a violation occurs.
 - Reference URL

URL to a document that describes the compliance control in more details. Many times these documents may be stored in a content management system.
 - Keywords

Keywords can be assigned to a rule so that you can control how data is organized in various reports.
7. Click **Next**.
 8. On the next screen, you select the method of providing the signature definition file. You can either load it by uploading a file, or enter the text directly into the UI.
 9. Enter Compliant and Non-Compliant Message. These are the messages that will be shown in regards to the evaluation. When a violation occurs, the Non-Compliant message will be the string describing the event under the Incident Management capabilities.
 10. Choose the columns that will be displayed along with violations. These columns should be defined as return columns in the signature definition
 11. Click **Next**.
 12. The next screen will allow you to test your rule. You can choose a target in your environment and click the **Run Test** button. Any issues with the rule will be displayed and you can resolve them before saving the rule.
 13. Click **Next**.
 14. The final page allows you to review everything you have configured for this rule. Ensure that everything is correct and click the **Finish** button to save the rule.

This newly crated rule does not function until it is associated to one or more compliance standards and those compliance standards are associated to targets. Once this association happens, the following is the workflow of this rule:

- The standard/rule combination gets transferred to and then evaluated on the Management Agent-side against a metric collected specifically for the Compliance Standard and target type to determine compliance.
- The evaluation generates violations (if any).
- Violations are uploaded to Cloud Control server, from where they are subsequently processed into violations in Management Repository tables.
- Violations are then viewable in compliance results pages and the Compliance Dashboard

Example WebLogic Server Signature

Using the rule creation wizard makes it simple to add a new rule, but the important part of the WebLogic Server signature rule is the signature definition. A signature definition consists of a list of managed beans (MBeans) and an XQuery expression. Managed beans represent the configuration data to collect. They define a type and the

attributes within the type to collect. They also declare which attributes to consider in determining whether there are violations. The XQuery expression defines the logic to use in evaluating the collected data for compliance. An XML example signature definition follows.

```
<SignatureDefinition>
  <MBeanList>
    <MBean scoreBase="true" mBeanType="ServerRuntime">
      <AttributeName>Name</AttributeName>
      <AttributeName>WeblogicVersion</AttributeName>
    </MBean>
  </MBeanList>
  <XQueryLogic>declare function
local:getServerRuntimesEqualToVersionWithPatch($targetData, $major as xs:integer,
$minor as xs:integer, $servicePack as xs:integer, $scrNumber as xs:string) {
  for $ServerRuntime in $targetData/DataCollection/ServerRuntime
  let $weblogicVersion := fn:replace($ServerRuntime/@WeblogicVersion,
  &quot;WebLogic Server Temporary Patch&quot;;, &quot;&quot;);
  let $majorVersion :=
    let $spaceParts := fn:tokenize(fn:substring-after($weblogicVersion,
  &quot;WebLogic Server &quot;), &quot;; &quot;);
    let $majorVersionParts := fn:tokenize($spaceParts[1], &quot;;\.&quot;);
    return
      $majorVersionParts[1] cast as xs:integer
  let $SP_MP :=
    if ($majorVersion = 8) then
      &quot;;SP&quot;;
    else
      if ($majorVersion >= 9) then
        &quot;;MP&quot;;
      else &quot;; &quot;;
  let $minorVersion :=
    let $spaceParts := fn:tokenize(fn:substring-after($weblogicVersion,
  &quot;WebLogic Server &quot;), &quot;; &quot;);
    let $minorVersionParts := fn:tokenize($spaceParts[1], &quot;;\.&quot;);
    return
      $minorVersionParts[2] cast as xs:integer
  let $servicePackVersion :=
    let $spaceParts := fn:tokenize(fn:substring-after($weblogicVersion,
  &quot;WebLogic Server &quot;), &quot;; &quot;);
    let $servicePackParts := fn:substring-after($spaceParts[2], $SP_MP)
    return
      if ($servicePackParts = &quot;;&quot;) then
        0
      else
        $servicePackParts cast as xs:integer
  where $majorVersion = $major and $minorVersion = $minor and $servicePackVersion =
  $servicePack and

  fn:contains(fn:upper-case($ServerRuntime/@WeblogicVersion), fn:upper-case($scrNumber
))
  return
  $ServerRuntime
};
for $server in
local:getServerRuntimesEqualToVersionWithPatch(/,10,0,1,&quot;;CR366527&quot;;)
|
local:getServerRuntimesEqualToVersionWithPatch(/,10,0,0,&quot;;CR366527&quot;;)
return &lt;Server
Name=&quot;;{fn:data($server/@Name)}&quot;;/&gt;;</XQueryLogic>
```

```
</SignatureDefinition>
```

Effectively, this definition collects the server name and WebLogic version of all runtime servers. Much of the definition iterates over the preciseness of the version-major and minor patch, service pack, CR number, and so forth. A violation occurs if any server has either of the stated patches (10.0.1 CR366527 or 10.0.0 CR 366527), in which case return the name of the server to be reported in violation. Hence, the rule definition must include a column to account for display of the server name. The version is irrelevant in the context of the display. Those alerted are interested only in which servers are in violation.

Important Prerequisite Steps to Use WebLogic Server Signature Rules

The following are some required steps that are specific to the version of WebLogic you are trying to monitor:

1. WebLogic versions earlier than 10.3.3: To enable data collection for the WebLogic Server signature-based rules on WebLogic Server targets earlier than v10.3.3, you need a copy of `bea-guardian-agent.war`. You can find a copy of this war file in your OMS installation's work directory:
`$T_WORK/middleware/wlserver_10.3/server/lib/bea-guardian-agent.war`
2. WebLogic Server v9 and v10.0: Install and deploy `bea-guardian-agent.war` to all servers in the domain. Do not change the context root. For more information on installing a web application, see:
<http://<host>:<port>/console-help/doc/en-us/com/bea/wlserver/core/index.html>
3. WebLogic Server v10.3 up to and including v10.3.2: Copy the war file from your OMS installation into each target's `$WL_HOME/server/lib` directory. Restart all the servers in the target domain.
4. WebLogic Server v.10.3.3 and higher: No action is required.

Additional Notes for WebLogic Server Signature Rules

- All rules are visible in the global rule library and are visible to all users.
- Once the compliance standard rule is created, it is not automatically evaluated. Users must associate a rule to a compliance standard before it can be used. Only when a compliance standard is associated with one or more targets will a rule evaluation occur. Rules cannot be evaluated directly.
- One rule can be associated to multiple compliance standards.
- Various attributes of a rule can be customized through the compliance standard this rule is associated with. These customizations occur in the Compliance Standard screens. One of these attributes that can be customized per compliance standard is the importance of the rule in relationship to this standard.
- Because the user-defined compliance standard rule is defined by a privileged user, only privileged users can modify the compliance standard rule. Violation results are available to all users.
- To share this user-defined compliance standard rule with other privileged users, provide the XML schema definition (using the Export feature) so they can import the compliance standard rule to their Management Repository.
- You can minimize scrolling when reading the Description, Impact, and Recommendation information by restricting the text to 50 characters per line. If more than 50 characters are needed, start a new line to continue the text.

- Look at the context-sensitive help for information for each page in the Compliance Standard Rule wizard for specific instructions.
- Look at the context-sensitive help for information for each page in the Compliance Standard Rule wizard for specific instruction.

27.4.7.3 Creating a Real-time Monitoring Compliance Standard Rule

To create a Real-time monitoring compliance standard rule to monitor for user actions that occur on a target such as file changes, user access, and process activity, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standard Rules** tab.
3. Click the **Create** button.
4. In the Create Rule popup, select Real-time Monitoring type.
5. Click **OK**.
6. On the next screen, you are asked to fill out several key attributes of the rule:
 - **Rule Name**
Provide a unique name for the rule.
 - **Rule Lifecycle State**
Set whether the state of this rule is development or production. Development means that the rule is still being defined or tuned and is not yet ready to be used on targets yet. After you promote a rule to production, you cannot change it back to development.
 - **Severity**
The rule can have a severity level, which could be Critical (serious issue if this rule is violated), Warning (not a serious issue if violated), or Minor Warning (a minor issue if violated). Severity impacts the compliance score along with the importance that may be set for this rule when it is added to a compliance standard.
 - **Applicable To**
Target type this rule works against.
 - **Entity Type**
A type of object that is part of a target being monitored. For example, for the Operating System (OS), entity type may be OS File, OS Process, or OS User. For Database, an entity type may be Database Table, Database Function, Database Procedure, or Database User.
 - **Target Property Filter**
You can specify specific target properties that determine which targets this rule can work against when it is associated with a compliance standard. These properties are Operating System, Target Lifecycle State, Target Version, and Target Platform. When you specify a target property filter for this rule, for instance for Linux OS, it will only be applicable to targets on Linux Operating System.
 - **Description**
Description of the rule

- **Rationale**
Text describing what this rule is checking and what the effect of a violation of this rule may be.
- **Details URL**
URL to a document that describes the compliance control in more details. Many times these documents may be stored in a content management system.
- **Message**
The message that will be used for the violation when an observation is determined to be unauthorized.
- **Clear Message**
The message that will be used for a previous violation after it is cleared.
- **Keywords**
Keywords can be assigned to a rule so that you can control how data is organized in various reports.

For additional information, see [Importance of Target Property Filters for a Real-time Monitoring Rule](#).

7. Click **Next**.
8. On the next page, you select the facets that are to be monitored for this rule. You can include facets that are already defined or create a new facet inline with this rule creation. A facet is simply a list of patterns to monitor. For instance, a list of files, user names, processes, and so on. Facets are discussed later in the section [Real-time Monitoring Facets](#).
9. Click **Next** after including existing facets or adding new facets.
10. On the next screen, you will choose the actions you want to monitor. The actions you choose will depend on what entity type you chose for the rule. For instance, for OS File Monitoring, you can watch for actions such as file create, modify, delete, rename, and so on. For OS User monitoring, you can watch for actions such as login, logout, SU, SSH, and so on. You must choose at least one action to monitor for a rule.

For additional information, see [Selecting the Types of Actions You Want to Monitor](#).

11. Click **Next**.
12. On the next screen, you can optionally configure filters for monitoring. Filters are used to limit when or under what conditions you want an action to be observed. For instance, if you are monitoring a file facet FILES1, you can add a filter so that only file changes done by a specific list of users are captured, or if the change happens during a certain time window, or a certain process is used to modify the file. Filters are also facets, just of different entity types. If you are monitoring OS File entity type, you can apply an OS User, OS Process, or Time Window facet as a filter. You can include an existing facet, or create a new facet inline with the rule creation. If you cancel the rule wizard, any facet you created inline will still exist in the facet library.

For additional information, see [Using Facets as Filters in Real-time Monitoring Rules](#).

13. Click **Next**.

14. On the next screen, you can configure several settings related to how the observations are handled when detected at the Management Agent.
 - Authorize Observations Manually
 - Authorize Observations Automatically using Change Request Management System
 - Collection Settings

For additional information, see [Configuring Audit Status](#) and [Controlling Observation Bundle Lifetimes](#).

15. Click **Next**.
16. On this screen you can review the settings of the rule.
17. Click **Finish** to save the rule and return to the rule listing page.

Importance of Target Property Filters for a Real-time Monitoring Rule

When creating a rule, you must choose a target type for the rule. Since the Real-time monitoring capabilities on the Management Agent have some dependencies on operating system and versions of operating systems, you must be allowed to set the criteria for a rule. The target may be different on a target type, so patterns in the facets may be different. For instance, Oracle Database on Microsoft Windows is not the same as it is on the UNIX operating system.

If target property filters are not set, all rule options are available then at target-cs association time, if a target's settings do not match, then that rule and facet is ignored. If you only set, for example, the platform name, but not version, then only the options that are common across all versions of the platform are available.

The list of facets that are selectable when creating a rule are filtered by the target properties that are set when a facet is created. For instance if you have a facet, FACET1, that works on Linux or HPUNIX and you create a rule for Windows, FACET1 will not be available to select for your rule. This applies both when selecting the monitoring facet or using a facet as a filter. However if you create a rule for either Linux or HPUNIX, FACET1 will be available because the criteria for the rule at least overlapped with that of the facet.

Using Facets as Filters in Real-time Monitoring Rules

When creating a rule, facets can be used in two ways. The first is to use the facet to specify what entities to monitor in the rule. The second is to use the facet as a filter to apply on top of activities detected by the Management Agent.

You can use the same facet as a monitoring facet in one rule and a filtering facet in another rule. The benefit is once you define a collection of patterns, for example to define your administrative users, you can use that collection in many ways without having to redefine the collection again.

Filters in rules are set up to reduce the observations that are captured and reported to Cloud Control. If there are no filters defined, then all observations related to the monitoring facet(s) selected in the rule are captured. When selecting a facet as a filter, the default is to only include observations that have attributes that match. The following example IT compliance control demonstrates an example for the filtering:

IT Control: Monitor all changes to critical OS configuration files by administrators during production hours.

To implement this IT control, you can create a compliance standard rule with the following:

1. Create a rule and select the file facet "Critical OS configuration files" for the monitoring facet that has patterns covering all critical OS configuration files.
2. Select "content change" as the action types to capture
3. Add an OS Users filter selecting facet "Administrators" that lists patterns describing all of the OS user accounts that are considered administrators.
4. Add a Time Window filter selecting facet "Production Hours" that lists patterns describing the times of the week that are considered to be production hours. For example, Every day 4am-2pm PST.

When the Management Agent sees any content change to the patterns in Critical OS configuration files, it will only report these changes back to Cloud Control if the change happened during production hours and if any user described in the Administrator's facet is the one making the change. Filters can also be inverted to monitor anyone not in the administrators group or for changes outside of production hours.

More details on how to use filters is described in the section above on Creating a Real-time monitoring rule.

Configuring Audit Status

Each observation can have an audit status. This audit status can change over time and be set manually or automatically by Cloud Control. The way audit statuses are managed is configured when creating or editing a real-time monitoring rule.

When creating a rule, on the settings page of the wizard, the user has an option of choosing whether all observations detected against this rule will get their audit status manually from the user or automatically using connector integration with a Change Request Management server.

When the user chooses to manually set audit status in a rule, there are two options available:

- Default Audit status can be set so that all observations that are found against this rule are by default unaudited, authorized, or unauthorized. Unaudited is the same as saying they have not been reviewed and there has been no determination of whether the observation is good or bad.
- The user can choose to choose an informational event during manual authorizations. This is used to create a new event of informational class in the Incident Manager when a new observation bundle occurs. Based on this event, an event rule could be created to send a notification based on the observation bundle or perform any other action the Incident Manager can perform.

If the user chooses to use automatic reconciliation using a Change Request Management server, then steps must be taken to set up the Cloud Control connector for Change Management. This is explain in detail in the later section, Additional Setup for Real-time Monitoring.

Once the connector has been configured, there will be a drop down in this settings step of the rule creation wizard to choose which connector to use for this rule. Based on attributes of the observation and observations defined in any open change requests, the observation will be automatically determined to be authorized if there are open matching change requests, otherwise it will be considered unauthorized.

When using automatic reconciliation, an additional option is available to specify that the details of any authorized observations should be annotated back into the change request in the Change Request Management Server that allowed the observation to be authorized.

Multiple observations can belong to the same Observation Bundle. Even though an observation is part of group, the determination of authorized vs. unauthorized is done for a single observation, not at the group level. If a group has at least one observation that is marked as "unauthorized", then the group is considered to be a "violation" and an event or incident can be raised for this group violation.

Controlling Observation Bundle Lifetimes

Observation bundles are logical groupings of observations that occur over a relatively short period of time against the same rule on the same target and by the same user. The last three factors cannot be configured by the user because they will be how the Management Agent groups observations before sending them back to the Cloud Control server.

The user creating the rule however does have three variables that they need to be able to configure:

1. **Idle timeout:** The amount of time after the user has no more activity from their last activity against a specific rule on a given target. The use case for this is that a user logs into a server, starts making a few file changes and then no more file changes are made after 15 minutes. This 15 minute waiting period is the idle timeout. After this idle timeout period is reached, the current observation bundle is closed and sent to the Cloud Control server. The next time a new observation is detected, a new group will be started and the process starts over.
2. **Maximum lifespan of a group:** If a user were to set the idle timeout to 15 minutes and a user on a host was making one file change every 10 minutes for an indefinite period of time (say through a script or even manual), the observation bundle will never close and therefore never get sent to the Cloud Control server for reporting/processing. Setting the maximum lifespan of a group tells the Management Agent to only allow a group to accumulate for a maximum specific time. For example, this maximum lifespan may be 30 minutes or an hour.
3. **Maximum number of observations in a bundle:** If a rule is being triggered because of an activity that is causing a lot of observations to be detected, it may be desirable for the user to not bundle every observation together if there are too many. Bundles have a management lifecycle to them where observations can be set to authorized/unauthorized, after they arrive at the Cloud Control server. Having observation bundles with tens of thousands of observations could become hard to manage.

The user creating a rule cannot choose to turn off bundling, but if they desired to reduce delays in observation reporting to Cloud Control server, they could set the idle timeout and maximum lifespan of a bundle to be lower.

The event/incident subsystem will track only the observation bundles, not each individual observation. If one observation is marked as unauthorized, then the entire bundle will be in violation. This bundle is the entity that will be tracked by the Incident Management event.

Observation bundles are built at the Management Agent and will only be sent to the Cloud Control server when the bundle is complete according to the above criteria. In most compliance use cases, this is acceptable because you will not need to view the results immediately. Capturing and bundling results together is more important for understanding what is happening and making observations easier to manage.

When an observation becomes part of two or more bundles on the Management Agent because the same facet is used in multiple rules or multiple targets on the same host monitor the same facet with shared entities, then whenever the first bundle either hits its ending criteria (idle timeout, group maximum life, or maximum group entries),

then all of the bundles containing these shared observations are closed at the same time.

To control observation bundle lifetimes, see the section above on how to create Real-time Monitoring Rules and set the appropriate settings on Settings page of the rule creation wizard.

Selecting the Types of Actions You Want to Monitor

When creating a rule, you can decide which types of observations or user actions are important to be monitored and reported back to Cloud Control. The Management Agent has a specific set of observations that are possible for each entity type. Some options may be specific to certain operating system platforms or versions. You can select one or more of these options.

The observation types that you may be able to select can also be limited by the target properties/criteria selected for the rule. For instance, some operating systems may not have every monitoring capability for files. When building the list of available observation types available, the target type, entity type, and target properties are all taken into consideration to come up with the resulting available observation types.

To select the type of observations you want to monitor in a rule, follow these steps:

1. If you want to select observations for a currently existing rule, click on the Real-time Monitoring rule in the Rules table and then click **Edit**.

Cloud Control opens the Edit Rule: Real-time Monitoring wizard and displays the Details page. Move to the Observations page.

If you want to select observations while creating a new rule, click **Create** to create a new rule. Cloud Control opens the Create Rule: Real-time Monitoring wizard and displays the Details page. After entering relevant information on the Details and Facets pages of the wizard, move to the Observations page.

2. On the Observations page, select one or more activities to be observed from the list that appears. During target association for this rule, auditing must be enabled to capture selected details. It is important to note that different operating systems and different capabilities have specific auditing requirements.
3. In the Parameters section, if there are additional observation parameters, you can review and update the parameters.

Additional Notes for Real-time Monitoring Rules

- All Rules are visible in the global rule library and are visible to all users.
- Once the compliance standard rule is created, it is not automatically evaluated. Users must associate a rule to a Compliance Standard before it can be used. Only when a compliance standard is associated with one or more targets will a rule evaluation occur. Rules cannot be evaluated directly.
- One rule can be associated to multiple compliance standards.
- Various attributes of a rule can be customized through the compliance standard this rule is associated with. These customizations occur in the Compliance Standard screens. One of these attributes that can be customized per compliance standard is the importance of the rule in relationship to this standard.
- Because the user-defined compliance standard rule is defined by a privileged user, only privileged users can modify the compliance standard rule. Violation results are available to all users.

- To share this user-defined compliance standard rule with other privileged users, provide the XML schema definition (using the Export feature) so they can import the compliance standard rule to their Management Repository.
- You can minimize scrolling when reading the Description, Impact, and Recommendation information by restrict the text to 50 characters per line. If more than 50 characters are needed, start a new line to continue the text.
- Look at the context-sensitive help for information for each page in the Compliance Standard Rule wizard for specific instructions.
- If you choose to monitor OS File entity type, you will notice one action type "File Content Modified (successful) - Archive a copy of the file [Resource Intensive]". If you select this option, every time a file modify action is observed, a copy of the file will be archived locally on the Management Agent. This can be used later to visually compare what changed between two versions of the file. There is an additional setting to set how many archived copies to store on the Actions to Monitor page of the rule creation wizard.
- When you add a facet inline with the create rule wizard either as a monitoring facet or as a filtering facet, if you cancel the rule wizard, the newly created facets will still exist and be usable in future rules. You can delete these facets by going to the facet library. Real-time monitoring facets are discussed in a separate section later in this document

27.4.7.4 Creating Like a Compliance Standard Rule

To create a compliance standard rule like another compliance standard rule, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standard Rules** tab.
3. Highlight the rule you want to replicate.
4. Click **Create Like** button.
5. Customize the fields as needed.
6. Click **Save**.

27.4.7.5 Editing a Compliance Standard Rule

To edit a compliance standard rule, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standard Rules** tab.
3. Highlight the rule you want to edit and click the **Edit** button.
4. Step through the screens of the rule creation wizard as previously described when creating a rule.
5. Click **Save**.

Usage Notes

- For repository rules, you can change all the rule properties except the Rule Name, State (if it is already production), and Applicable To.

For real-time monitoring rules, you cannot change Rule Name, State (it is already production), Applicable To, Target Property Filters, and Entity Type.

- If you change the critical rule properties for a repository rule, for example, rule query, violation condition, parameters, or severity, then editing the rule invalidates the results for compliance standards which refer to the rule. The compliance standards compliance score will be reevaluated at the next rule evaluation.
- For rules in production mode, you have a choice to create and save a draft of the rule or to overwrite the existing production rule. If you create a draft, you can edit the draft rule, at a later point in time, test it, and then overwrite and merge it back to the original production rule the draft was made from. **Note:** You cannot include a draft rule into any compliance standard.
- For WebLogic Server Signature rule or Real-time Monitoring rule, if the rule being edited is referred to by a compliance standard which is associated with a target, then the rule definition will be deployed to the Management Agent monitoring the target, so that the Management Agent can evaluate the latest definition of the rule. In the case where the Management Agent is down or unreachable, the rule definition changes will be propagated to the Management Agent as soon as the Management Agent is available.

27.4.7.6 Deleting a Compliance Standard Rule

Before you delete a rule, you must ensure that compliance standard rule references have been removed from compliance standards before deleting the compliance standard rule. You cannot delete a rule that is in use by a compliance standard.

To delete a compliance standard rule, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standard Rules** tab.
3. Highlight the rule you want to delete, click **Delete** button.
4. Confirm that you want to delete the rule by clicking **OK**.

27.4.7.7 Exporting a Compliance Standard Rule

The Export feature provides a mechanism for transporting user-defined compliance standard rule definitions across Management Repositories and Cloud Control instances. The export stores the definitions in an operating system file. Because the exported compliance standard rule definitions are in XML format, they conform to the Oracle Compliance Standard Definition (XSD) format. You can then change the definition of the compliance standard rule and re-import the generated compliance standard rule definitions into another Management Repository.

To export a compliance standard rule, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standard Rules** tab.
3. Highlight the rule you want to export.
4. From the **Actions** menu, select **Export**.
5. Provide the file name to which the standard rule is to be exported.
6. The XML representation of the compliance standard rule is generated and placed in the directory and file you specified.

27.4.7.8 Importing a Compliance Standard Rule

Importing allows you to re-use a compliance standard rule that you already have, share rule definitions across multiple instances of Cloud Control, or enable offline editing of the rule.

Before you import a compliance standard rule, ensure the compliance standard rule to be imported is defined in a file. The file should be locally accessible to the browser you are using to access Cloud Control. Also ensure that you have privileges to access the compliance standard rule definition XML file to be imported.

To import a compliance standard rule, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standard Rules** tab.
3. From **Actions** menu, select **Import**.
4. Provide the file name from which the rule definition (as per Compliance Standard Rule XSD) will be imported. Specify whether to override an existing definition if one already exists. The override option is not available to Real-time monitoring rules.
5. Click **OK**.

27.4.7.9 Browsing Compliance Standard Rules

To browse compliance standard rules, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standard Rules** tab.
3. To view the details of a particular standard rule, highlight the rule and click **Show Details**.

27.4.7.10 Searching Compliance Standard Rules

To search for compliance standard rules, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Click the **Compliance Standard Rules** tab.
3. In the Search portion of the page, provide criteria to use to narrow the search.

By default, all the compliance standard rules in the compliance standard rule library appear in the results table. However, you can specify a set of search criteria and then perform a search that will display only the compliance standard rules that meet those criteria in the results table.

For example, if you choose Security in the Category list, contains in the Compliance Standard Rule list, "port" in the adjacent Compliance Standard Rule text field, Host in the Target Type list, and then click **Go**, Cloud Control displays only the compliance standard rules for the host security category that contain "port" in their names.

4. Click **Search**.

27.4.7.11 Compliance Standard Rules Provided by Oracle

Oracle provides over 1600 compliance standard rules.

27.5 Real-time Monitoring Facets

The real-time monitoring rule definition includes facets that are used to determine what is important to monitor for a given target type, target properties, and entity type. A facet is a collection of patterns that make up one attribute of a target type.

The following sections explain real-time monitoring facets in detail:

- [About Real-time Monitoring Facets](#)
- [Operations on Facets](#)

27.5.1 About Real-time Monitoring Facets

A target type has several facets to it. A target type will have a facet of which files are critical configuration files, which files are log files, which files are executables, which database tables have sensitive configuration data, and so on. The sum of all of these facets for a given target type makes up everything that is important to monitor for the given target type in terms of compliance.

For a given target type, you can create any number of facets. A facet is not only for a specific target type, but for a specific target type plus a combination of some number of target type properties. For instance, creating a facet for a Host Target Type on Windows is different than creating a facet for a Host Target type on Linux. A facet can have several target type properties or can be open to any target without specifying any properties.

Facets are reusable in many rules. The benefit is that you can add or remove entries from a facet without having to modify every rule. For instance, if today there are 5 log files you want to monitor, you can setup your rules to monitor a facet listing those 5 files. When a new log file should be added tomorrow, you only need to change the facet, not each rule.

Facets can be created on their own, or created inline with a Real-time Monitoring rule creation. No matter how they are created, they can be used again at a later time in any number of rules.

Real-time Monitoring facets based on target types are used to specify the entities to monitor in real-time monitoring rules. As an example, if monitoring a host for file changes, a facet can be a list of distinct single files, patterns with wildcards that would include many files, or simply an entire directory. These patterns can also include parameters that have a default, but can be overridden as needed for each target. Built-in parameters, such as ORACLE_HOME will be dynamically filled in for each target. If you wanted to specify monitoring the database configuration file *tnsnames.ora*, your pattern may be `{ORACLE_HOME}/network/admin/tnsnames.ora`.

Facets can be used in two totally distinct ways. Primarily, facets describe what to monitor. In the rule creation wizard, these facets are selected on the wizard step "Entities to Monitor". Facets also can be used to filter your monitoring results. These filtering facets are specified on the Filters step of the rule creation wizard. When monitoring an OS file entity type for instance, you can filter your results based on the user that made a file change, the time the file change happened, or the process used to make the file change.

When performing continuous real-time monitoring, it is important to scope your monitoring only to critical entities. Monitoring more activity than is important to the organization will result in higher CPU loads on the Management Agent as well as a very large amount of data to be processed/stored by the Oracle Enterprise Manager servers.

27.5.1.1 Facet Entity Types

Each facet has an *entity type* which defines what kind of entities the facet describes. For example, for OS level monitoring, there are OS File, OS Process, OS User, Windows Registry, and several Active Directory entity types. For database monitoring, the entity types include Table, View, Index, Procedure among others. The possible entity types are fixed by the continuous real-time configuration change monitoring capabilities available from the Management Agent.

Creation of facets is possible through the Facet Library screen. In this screen, you can add/edit patterns for facets, and see which facets are being consumed by rules.

The following table lists the entity types Cloud Control supports for real-time monitoring:

Table 27–2 Monitored Entity Types

Entity Types		
OS File	Oracle Database Table	Oracle Database Package
OS Process	Oracle Database View	Oracle Database Library
OS User	Oracle Database Procedure	Oracle Database Trigger
Microsoft Windows Registry	Oracle Database User	Oracle Database Tablespace
Microsoft Active Directory User	Oracle Database Index	Oracle Database Materialized View
Microsoft Active Directory Computer	Oracle Database Sequence	Oracle Database Cluster
Microsoft Active Directory Group	Oracle Database Function	Oracle Database Link
Oracle Database Dimension	Oracle Database Profile	Oracle Database Public DB Link
Oracle Database Synonym	Oracle Database Public Synonym	Oracle Database Segment
Oracle Database Type	Oracle Database Role	Oracle Database SQL Query Statement

27.5.1.2 Facet Patterns

A facet contains one or more patterns. These patterns can express inclusion or exclusion filters. For instance, you may define a facet for critical configuration files that looks like the following:

Include c:\myapp1\config

Exclude c:\myapp1\config\dummy.cfg

In this case, everything under c:\myapp1\config will be considered to be a member of this facet except for the individual file c:\myapp1\config\dummy.cfg. In general there are some rules to how patterns work given the most common use cases listed below. Each entity type might have special cases or special formats of patterns.

- Patterns of the same specificity with one being include and one being exclude, the include will win.
- Patterns that are more specific override (like in the above example, exclude dummy.cfg overrides the inherited include c:\dummy.cfg from the first pattern.)
- If there are no patterns at all, exclude * is assumed (for example, no entities in the facet)

For each pattern that you add to a facet, an optional description field is available to let you document their patterns.

27.5.2 Operations on Facets

The following sections explain the operations you can perform on facets:

- [Viewing the Facet Library](#)
- [Creating and Editing Facets](#)
- [Creating and Editing Facet Folders](#)
- [Deleting a Facet](#)
- [Using Create Like to Create a New Facet](#)
- [Importing and Exporting Facets](#)
- [Changing Base Facet Attributes Not Yet Used In a Rule](#)

Ensure you have the privileges to create, delete, and modify facets as these configurations relate to the compliance monitoring. See [Section 27.1.3, "Privileges and Roles Needed to Use the Compliance Features"](#) for information.

27.5.2.1 Viewing the Facet Library

Any user who can view observation data is able to also view the facet library and see the facet history for any facet.

There are two ways to view the facet library, search mode and browse mode. In search mode, all facets meeting the search criteria are shown in a flat list. In browse mode, facets are shown along with a folder hierarchy that the facets belong to. This folder structure can help users manage a very large number of facets in Cloud Control.

To view the facet library in search mode, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Choose the Real-time Monitoring Facets Library tab.

Cloud Control displays the Facet Library page that lists all existing facets along with their target type, entity type, and other details about the facet. From this page you can perform administrative tasks such as create, create like, view, delete, import and export if you have the audit author role.

3. Click the **Search Facets** tab.

The Facet Library page displays the Facet Name, Author, Target Type, Entity Type, Rules Using the facet, Description, and the Last Updated time of the facet. You can see the details of any facet by selecting it from the table and clicking Show Details.

4. You can choose which columns to display in the table by clicking **View** and then choosing **Columns**. You can either choose to **Show All** columns or you can select individually the columns you want to appear in the table. You can reorder the columns by clicking Reorder after you click View and then changing the order in which the columns appear by moving them up or down using the arrow keys.
5. You can expand the area of the page titled "Search" to choose the search criteria to apply to the view of facets.
6. You can view a history of a selected facet by choosing it from the table and then clicking History. The View History page appears.

To view the facet library in browse mode, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Choose the **Real-time Monitoring Facets Library** tab.

Cloud Control displays the Facet Library page that lists all existing facets along with their target type, entity type, and other details about the facet. From this page you can perform administrative tasks such as create, create like, view, delete, import and export if you have the audit author role.

3. Click the Browse Facets tab.

The Facet Library page that is shown is split into two views, The left side shows the facet folder hierarchy. The right side lists facets in the folder that is selected on the left. The table on the left displays the Facet Name, Author, Target Type, Entity Type, Rules Using the facet, Description, and the Last Updated time of the facet. You can see the details of any facet by selecting it from the table and clicking Show Details.

4. You can choose which columns to display in the table by clicking **View** and then choosing **Columns**. You can either choose to **Show All** columns or you can select individually the columns you want to appear in the table. You can reorder the columns by clicking **Reorder** after you click View and then changing the order in which the columns appear by moving them up or down using the arrow keys.
5. The only filtering allowed on this screen is by selecting a different folder. You will always see the facets that are in the selected folder only.
6. You can view a history of a selected facet by choosing it from the table and then clicking **History**. The View History page displays.

27.5.2.2 Creating and Editing Facets

When you create a facet and subsequently use a facet in a Real-time Monitoring Compliance Standard Rule, the compliance rule only references the facet. If the content changes, then the rule will use the new content automatically.

The content of the facet only begins being used when it is added to a rule that is part of a compliance standard that is associated to one more targets.

Each facet is assigned a description that allows you to document the facet. Each pattern also has an optional description field. only begins being used when it is added to a rule that is part of a compliance standard that is associated to one more targets.

To create or edit a facet, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Choose the **Real-time Monitoring Facets Library** tab.

Cloud Control displays the Facet Library page that lists all exiting facets along with their target type, entity type, and other details about the facet. From this page you can perform administrative tasks such as create, create like, view, delete, import and export. There are two views when looking at this page, search or browse. In the search view, all facets are listed in a flat list. In the browse view, facets are grouped in folders to make it easier to find facets.

3. Click **Create** to create a new facet.
4. Choose which facet folder this facet should belong to. If you have not yet created the folder for it, you can add it to the Unfiled folder. This folder always exists and cannot be remove. Later you can move the facet to a new folder you create using drag-and-drop in the UI from the Unfiled folder to the new folder.

5. Enter the name you want to assign to the facet in the **Facet Name** field, then choose the target type for the facet you are creating from the drop-down list in the **Target Type** field. Once you choose the Target Type, you can enter values in the Target Property Filter fields.

The target properties you add here limit which targets to which this facet can ultimately be assigned. For instance, you could define a facet to work only for Linux version 5 on 64-bit servers.

6. Choose the **Entity Type** from the drop-down. This list will be limited depending on the target type chosen previously.
7. Enter a description for the facet in the **Description** field.
8. The Create Facet page contains two tabs you can use to enter the patterns and parameters for the facet you create. Use the Patterns tab to add patterns to be either **Included** or **Excluded**. Use the **Add** or **Delete** buttons to add additional patterns or to remove a selected pattern from the facet definition. There is a bulk add button which will bring up a popup window where you can paste text listing patterns rather than entering each in the UI manually.
9. If you are defining a facet for the OS File entity type, there is an optional ability to browse a host to find the files you want to monitor. The right side of the page has an area where you can choose the host to use as the basis for looking for files. In the pattern area, you can click the Browse button to interactively browse the files on the selected host and select the files to include in the pattern. After selecting patterns from a host, you can continue to manually add more or edit existing ones.
10. Use the Parameters tab to view parameters that are part of the new facet. Oracle provides a set of predefined parameters based on target parameters (such as ORACLE_HOME) that are defined out of the box. These parameters do not require a default value and are always set according to the target's value. Parameters will appear under this tab when they are used in a pattern. To start using a new parameter, simply add the parameter to the pattern by enclosing it in curly brackets {}. For instance, a pattern of {INSTALL_DIR}\config\main.conf would result in a parameter of INSTALL_DIR being listed under this tab. All parameters must have a default value that will be automatically used for all targets against which this facet is used. This value can be overridden when associating a compliance standard containing a real-time monitoring rule to one or more targets. The Parameters tab displays the Parameter Name, Default Value, Used in Pattern, and Description. Used in Pattern indicates that the parameter is currently in use. This parameter may have been defined at some point in a pattern and then removed. The pattern will still be available for use again at a later time even if the pattern is not currently in use. If the entity for which you are adding a pattern includes a "{" or "}", you can escape these characters by using "{{}" and "}}" in the pattern respectively. These will not be counted as parameters.
11. A third tab, Time Window is only available if the facet being created/edited is of entity type Time Window. A facet of this entity type is only usable as a filter in a Real-time monitoring rule. For instance, you can specify in the rule that you only want to monitor a facet during a specific time, for example, "Production Hours". In the Duration section, choose either a **24 Hour Interval** or **Limit Hours to**, which allows you to enter a Start time and an Interval in Hours and Minutes. In the Repeating section, you can choose either *All the time* or you can select **Repeat** and then choose which days of the week to repeat the operation.
12. Choose **OK** to create the facet.

27.5.2.3 Creating and Editing Facet Folders

When viewing the facets in Browse Facets mode, you will see two regions on the page. The left side will show the facet folders which exist. The right side will show the facets that exist in the currently selected folder.

On the left side showing the folders, there are three actions available for folders.

- **Create:** Allow you to create a new folder. A popup will display asking for the folder name to create. You will also have the choice of making this new folder a top level folder or adding it as a child to the currently selected folder.
- **Rename:** Allows you to rename an existing user-defined folder
- **Delete:** Allows you to delete a user-defined folder. You cannot delete a folder that has facets or other folders inside of it.

You cannot delete, rename or move out-of-the-box folders that are populated by Oracle.

There is a default folder that exists called Unfiled. Anytime a facet is created or imported without specifying a folder, it will go into this Unfiled folder.

You can move facets into folders by simply finding the facet you want to move in the right side, selecting it and dragging it to the folder on the left where you want to place it. The facet will move to that folder. A facet can only belong to one folder at a time and it always must belong to a folder (even if it is just the Unfiled folder). You can also click on the facet and click on the MOVE button. A popup window will appear letting you choose which folder to move the facet to.

Folders have no impact on observation analysis or compliance score. They are only used in the Real-Time Monitoring Facets library screen to make it easier to manage a very large number of facets that exist.

27.5.2.4 Deleting a Facet

Deleting a facet is not possible as long as the facet is in use either as a monitoring facet in a rule or as a filter facet in a rule. If this facet is not in use in any rules, then the facet can be deleted. If a facet is in use, the user is alerted to the current use and not allowed to delete the facet until the rules using it are modified to no longer include it.

When deleting a facet, any historic observation data will no longer be referenced to the facet and instead it will show "(Deleted Facet)" as the name of the facet to which it is related. This observation data will only be available through the Search Observations page, not the Browse pages.

For compliance-focused users, customers typically would want to keep the unused facet available so the compliance data is not lost. You can also remove the patterns as long as you keep the actual facet to maintain collected observations. Then only after the compliance data related to this old facet is no longer available, you can delete the facet without any data loss.

To delete a facet, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Choose the **Real-time Monitoring Facets Library** tab.

Cloud Control displays the Facet Library page that lists all existing facets along with their target type, entity type, and other details about the facet. From this page you can perform administrative tasks such as create, create like, view, delete, import and export.

3. Select the facet from the list of facets in the table on the page.

4. Click **Delete** to delete the facet. You will be prompted to confirm that you want to delete the facet.

27.5.2.5 Using Create Like to Create a New Facet

Facets that ship with the product or with a plug-in cannot be changed. If you want to enhance or modify the out-of-box content, you must use the create-like functionality to make your own copy of the facet which can then subsequently be edited.

An important limitation to the Create Like function is that you cannot change the target type or entity type. The patterns contained in the facet may be dependent on target type or entity type. If you want to use Create Like and change these attributes, you should use Export to export the original facet, edit the name, target type, entity type in the XML, and then import as a new facet.

To use create like to create a new facet, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Choose the **Real-time Monitoring Facets Library** tab.

Cloud Control displays the Facet Library page that lists all existing facets along with their target type, entity type, and other details about the facet. From this page you can perform administrative tasks such as create, create like, view, delete, import and export.

3. Choose the facet from the facet table that you want to use as the basis for the new facet you want to create.
4. Click **Create Like**.

Cloud Control displays the Create Facet page. All the values that were applicable to the facet you want to clone are entered. Use the page to edit the values for the new facet and click **OK**.

It is important to understand that if the original base facet you used in the create like activity is changed, that change will not be reflected in the newly created facet. There is no relationship maintained when using Create Like.

5. For more information about using the Create Facet page, see [Section 27.5.2.2, "Creating and Editing Facets"](#).

27.5.2.6 Importing and Exporting Facets

You can select facets and export or import them. All selected facets will be exported into one output file.

On import, if a facet of the same name/target type/entity type combination already exists, the import fails with an error that the facet already exists. The user must change the import file to remove the duplicate name and retry the import.

The combination of name, target type, and entity type define a unique facet. You can have the same name facet across different target types and entity types.

To export a facet, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Choose the **Real-time Monitoring Facets Library** tab.

Cloud Control displays the Facet Library page that lists all existing facets along with their target type, entity type, and other details about the facet. From this page you can perform administrative tasks such as create, create like, view, delete, import and export.

3. Select one or more facets from the list of facets on the Facet Library page that you want to export and then click **Export**.
4. On the Open dialog box, you can choose to open or save the facet xml file using an XML editor of your choice and then either edit or save the file to another location.

To import a facet, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Choose the **Real-time Monitoring Facets Library** tab.
Cloud Control displays the Facet Library page that lists all existing facets along with their target type, entity type, and other details about the facet. From this page you can perform administrative tasks such as create, create like, view, delete, import and export.
3. Click **Import** and choose the facet XML file you want to import into the Facet Library.
4. Cloud Control imports all facets specified in the imported XML file. You can then edit the facet or use any other action on it as you would any other facet in the library.

27.5.2.7 Changing Base Facet Attributes Not Yet Used In a Rule

After a facet is in use in at least one rule (either as a monitoring facet or as a filter facet), you cannot change the facet name, target type, entity type, or target criteria of the facet since the rules that have been created are already bound to these attributes. The only attributes that can be changed are the facet patterns, parameters and description fields. Although the rule is not dependent on the facet name, users have used them in their rules based on the name of the facet. Allowing the name of the facet to change after consumption will only lead to confusion of the rule authors when analyzing compliance results and observations of the rule authors.

If a facet is not currently in use but has been in use in the past, then it is treated the same as an in-use facet since the historic observation data will still be tied to the past facet.

You cannot make changes to the out-of-box facets that ship with the Cloud Control product. If you want to use an out-of-box facet with changes, you can perform a "Create Like" operation and then modify the newly created facet as needed.

To change base facet attributes, follow these steps:

1. From the **Enterprise** menu, select **Compliance**, then select **Library**.
2. Choose the **Real-time Monitoring Facets Library** tab.
Cloud Control displays the Facet Library page that lists all existing facets along with their target type, entity type, and other details about the facet. From this page you can perform administrative tasks such as create, create like, view, delete, import and export.
3. Choose the facet from which you want to create a new facet with modified attributes. Click **Create Like**.
4. Enter a new Facet Name and change whatever attributes to create a new facet based on the previous facet.

27.6 Example of Creating Repository Rule Based on Custom Configuration Collections

This example illustrates how a compliance rule can be created and run on a custom configuration which collects a sample configuration file (for this example, /tmp/foo.xml) for targets of type Host.

For this example, create a sample /tmp/foo.xml file with following contents:

```
<some_config>
  <prop foo="1" />
  <prop bar="2" />
</some_config>
```

The steps include how to:

- Create a custom configuration
- Create a custom-based repository rule
- Create a compliance standard
- Associate a target
- View results

To create a custom configuration:

The following steps describe how to create a custom configuration.

1. From the Enterprise menu, select **Configuration**, then select **Custom**.
2. From the Custom Configurations page, click **Create**. The Create Custom Configuration page appears.
 - a. Type the Name (for example, compliance_ccs), a description (optional), select Target Type (for this example, Host).
 - b. In the Files & Commands section, type the Default Base Directory. [Use /tmp as the directory.]

This is an example. For a real target it should be the directory containing the target's configuration files.

Note: All files collected by custom configurations MUST NOT change on a daily basis, but should only change very rarely due to an explicit action by an administrator.

- c. Click **Add**.
 - In the Type column, select **File**.
 - In the File/Command column, type **foo.xml**. The Alias column is automatically filled in with foo.xml.

Note: You can use any file or files, not just xml and not just "foo.xml" expressions. Custom configuration supports many files and corresponding parsers.

 - In the Parser column, select **XML Parser (default)**.
- d. Click **Add** again.
 - In the Type column, select **File**.
 - In the File/Command column, type **foo.xml**. The Alias column is automatically filled in with foo.xml.

- In the Parser column, select **XML Parser (default)**.
- e. Click **Save** located at the bottom of the page.
- 3. In the Custom Configurations page, highlight `compliance_css` and click **Deploy**. The Deployments page appears.
 - a. Click **Add** to select targets on which CSS needs to be deployed.
 - b. On the Search and Select: Targets page, highlight the host target where file `/tmp/foo.xml` was created and click **Select**.
 - c. Click **Apply** on the Deployments page.
- 4. On the Submit Pending Deployment Actions popup, select **Yes**. This action will submit the deployment action.

On the Deployments page, click **Refresh Status** to refresh the status of the deployment until the Status column displays "Successfully deployed".
- 5. Now that deployment is submitted, click **Cancel** to exit the page. (**Note:** Clicking Save instead of Apply earlier, would have exited the page right after the submission of the deployment action.)

To create a custom-based repository rule based on custom configuration collection:

1. From the Enterprise menu, select **Compliance**, then select **Library**.
2. On the Compliance Library page, click the **Compliance Standard Rules** tab.
3. Click **Create**.
 - a. On the Create Rule popup, select **Repository Rule** and click **Continue**.
 - b. On the Create Rule: Repository Rule: Details page, type in the Rule name, for our example, `compliance_css_rule`.
 - c. For the Compliance Rule State, select Development, then select Minor Warning for the Severity. For Applicable To: select Host. Click Next located at the top-right of the page.
4. On the Create Rule: Repository Rule: Check Definition (Query) page, click **Model Query**. New Search Criteria page appears.
 - a. Select `compliance_css` (Parsed Data) from the Configuration Item menu under "Commonly Used Search Criteria".
 - b. Under the Host section and Parsed Data subsection, type `foo.xml` for Data Source contains. For the Attribute, select **is exactly** comparison operator and type `foo` to refer to the "foo" attribute in our sample file. (**Note:** % sign can also be used as a wild card character in these expressions for Data Source and Attribute.)
 - c. Click **Search** to see the rows returned for this filter. A table displays the data with value 1 for attribute foo in our file.
 - d. Click **OK**.
 - e. The Create Rule: Repository Rule: Check Definition (Query) displays again but this time the SQL Source appears.
 - f. Click **Next**. **Note:** In general, you could also update the query before proceeding, if needed.

5. The Create Rule: Repository Rule: Check Definition (Violation Condition) page displays.
 - a. Check all the columns as Key columns (VALUE, ATTR, CONTAINER, and DATA SOURCE NAME), except the INFO column.
 - b. In the Condition Type section of the page, select Simple Condition, and in the Column Name select VALUE and change the Comparison Operator to equal sign (=). In the Default Value column, type 1. Click **Next**.
6. In the Create Rule: Repository Rule: Test page, click the icon next to Target Name field. The Search and Select: Targets popup appears. Find the host where the custom configuration was deployed. Select it and click **Select**.
7. In the Create Rule: Repository Rule: Test page, click **Run Test**. When the test runs successfully, you get a confirmation stating that the Run Test - Completed Successfully.

You should see one violation after running the test because we specified value of "1" in step 5 above for violation condition and our sample file had value "1" for attribute foo. Click **Close**.
8. On the Create Rule: Repository Rule: Test page, click **Next**.
9. In the Create Rule: Repository Rule: Review page, ensure that all the information that you added is correct. Click **Finish**.

To create a compliance standard:

1. From the Enterprise menu, select **Compliance**, then select **Library**.
2. Click the Compliance Standards tab and click **Create**.
3. On the Create Compliance Standard popup, type **compliance_css_cs** in the Name field, select **Host** from Applicable To menu, and select Repository as the Standard Type. Click **Continue**.
4. The compliance standard page displays with the information regarding the compliance_css_cs compliance standard. Right-click on compliance_css_cs on the left side and select the **Add Rules...** option in the right-click menu.
5. On the Include Rule Reference popup, select compliance_css_rule. Click **OK**. Click **Save** to save the compliance_css_cs.
6. A confirmation message appears on the Compliance Library page stating that the compliance standard has been created. Click **OK**.

To associate targets:

1. Select the compliance_css_cs that was just created. Click **Associate Targets**.
2. On the "Target Association for Compliance Standard: compliance_css_cs" page, click **Add** to add targets.
3. On the Search and Select: Targets page, select a target where /tmp/foo.xml is present and click **Select**. Click **OK**.

You will then be prompted whether you want to Save the association or not. Click either Yes or No. You will then get an Informational message stating that the compliance standard has been submitted to the target for processing.

To view Results:

1. From the Enterprise menu, select **Compliance**, then select **Results**.

On the Compliance Results page, select the `compliance_css_cs` compliance standard and click **Show Details** to view the details of the compliance standard created.

2. Click the **Violations** tab associated with the `compliance_css_rule`. The target is associated with one violation.
3. Click on the rule node in the tree to see the **Violation Events** tab, then click on this tab to see the violation details for the rule. Click on a violations row in the violations table, to view details of the violation.

Managing Database Configuration Changes

This chapter introduces database change management solution in the following sections:

- [Overview of Change Management for Databases](#)
- [Overview of Schema Baselines](#)
- [Overview of Schema Comparisons](#)
- [Overview of Schema Synchronizations](#)
- [Overview of Change Plans](#)
- [Overview of Data Comparison](#)

28.1 Overview of Change Management for Databases

To manage the lifecycle of enterprise applications, an organization will need to maintain multiple copies of an application database for various purposes such as development, staging, production, and testing. Each of these databases must adhere to different processes. For example, for production databases, it is essential to ensure adherence to proper production control procedures. It is vital that administrators have the tools to detect unauthorized changes, such as an index being dropped without the requisite change approvals. In such cases, monitoring changes to production databases day over day or week over week becomes vital.

Database compliance, that is, ensuring that all databases meet the gold standard configuration, is another important aspect of life cycle management. Compliance with organizational standards or best practices ensures database efficiency, maintenance, and ease of operation.

On development databases, developers make changes that the database administrator needs to consolidate and propagate to staging or test databases. The goal is to identify the changes made to development and then make the same changes to staging or test databases taking into account any other changes already in production database.

Typically, most applications will get upgraded over time. Also, most applications are customized by the business user to suit their needs. Application customizations are usually dependent on database objects or PL/SQL modules supplied by the application vendor. The application vendor supplies the upgrade scripts and the customer has very little transparency about the impact of the upgrade procedure on their customizations. When customers test upgrade databases, they can capture a baseline of the application schema before and after the upgrade. A comparison of the before and after baselines will tell the user what modules were changed by the application. This gives them a better idea about how their customizations will be impacted as a result of upgrading their application.

The following are core capabilities of Change Management that allow developers and database administrators to manage changes in database environments:

- Schema Baseline—A point in time of the definition of the database and its associated database objects.
- Schema Comparison—A complete list of differences between a baseline or a database and another baseline or a database.
- Schema Synchronization—The process of promoting changes from a database definition capture in a baseline or from a database to a target database.
- Schema Change Plans—A means of deploying specific changes from a development environment to one or more target databases.
- Data Comparison—A list of differences in row data between two databases.

For database versions 9.x and above, the user logged into the database target through Cloud Control must have `SELECT ANY DICTIONARY` privilege and `SELECT_CATALOG_ROLE` role for capturing or comparing databases. In addition to the `SELECT ANY DICTIONARY` privilege and `SELECT_CATALOG_ROLE` role, the user logging into the destination database for creating schema synchronization needs to be a database administrator (DBA) or must have appropriate privileges on the objects being synchronized and also the Execute Command Anywhere target privilege. To create or delete change plans, Cloud Control users need the Manage Change Plans resource privilege, `EM_ALL_OPERATOR` privilege, `VIEW` and `CONNECT` privilege for the targets, and Create resource privilege for the job system and Create new Named Credentials resource privilege. Users can also be granted View and Edit privileges on specific change plans.

When submitting a data comparison job, the user whose credentials are specified for the reference and candidate databases must have `SELECT` privilege on reference and candidate objects respectively. Additionally, the users needs these privileges: `SELECT ANY DICTIONARY`, `SELECT_CATALOG_ROLE`, and `CREATE VIEW`. When comparing objects with LOB type columns included, the users need to be granted `EXECUTE` privilege on `SYS.DBMS_CCRYPTO` package, since cryptographic hash value of the columns will be compared instead of actual column values. And in case you specify the comparison to be performed as of a time stamp or system change number (SCN), the users must also be granted `FLASHBACK` privilege directly on the reference and candidate objects in their respective databases.

Further, the user whose credentials are specified as reference database credentials must be a DBA with `EXECUTE` privilege on `DBMS_COMPARISON` program and in case the reference database is not the same as candidate database, the `CREATE DATABASE LINK` privilege as well.

Database link, comparison definitions, and views may be created in the reference database by the data comparison job. Views may be created in the candidate database. These objects created during the comparison processing will be dropped when the comparison is deleted, unless you specify the option to skip dropping them at the time of deletion.

Data comparison cannot be performed connecting to a remote candidate database as user `SYS` since `SYS` credentials cannot be used over database links.

28.2 Overview of Schema Baselines

A schema baseline contains a set of database definitions captured at a certain point in time. Baselines are stored in the Cloud Control repository as XML documents.

Each baseline must be assigned a unique name. A good practice to name baselines is to match it on the scope of the database objects being captured in the baseline, for example, Financial 11.5.10 or HR Benefits or PO Check Print. A baseline can have a series of versions that have been captured at different points in time. Creating multiple versions of a baseline allows you to track changes to the definitions of a set of database objects over time. You can compare two versions of the same baseline to see the changes that have occurred between them.

When creating a baseline, you also create a corresponding baseline scope specification, which describes the names and the types of database objects and schemas from which they should be captured. When you have created the baseline definition, you can then capture the first version of the baseline by submitting an Cloud Control job. At a later time, or at regular intervals, you can capture additional versions of the same baseline. Each baseline version records the metadata definitions as they exist at the time the version is captured.

Change management schema baselines are retained in the system until you delete them. When you delete a baseline, it is deleted from the system permanently. Delete operation cannot be undone. However, if a baseline may be needed in future, you can first export the baseline to a dump file (created on the repository database server host) and then delete the baseline. Baseline can then be imported back from the file at a later time if needed.

28.2.1 Overview of Scope Specification

A scope specification identifies the database objects to be captured in a baseline. (Scope specifications also identify objects to process in schema comparisons and synchronizations.) Once you have specified the scope of a baseline, you cannot change the scope specification. This restriction ensures that all versions of the baseline are captured using the same set of rules, which means that differences between versions result from changes in the database, not scope specification changes. To capture schema objects using a different scope specification, you must create a new baseline.

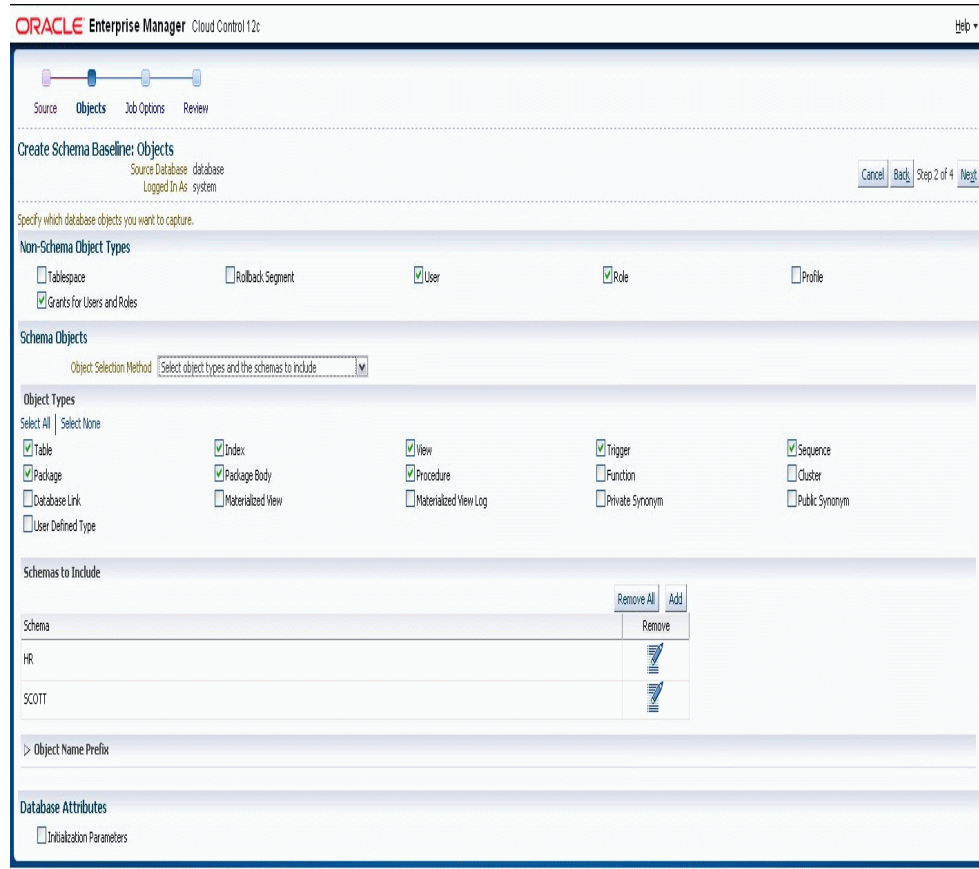
Baseline scope specifications take three forms.

- You can specify schemas and object types to capture. For example, you can capture all Tables, Indexes and Views in schemas APPL1 and APPL2. This form of scope specification is appropriate when there is a well-defined set of schemas that contain your application objects. In addition to schema objects, you can also capture non-schema objects (such as Users, Roles and Tablespaces) and privilege grants to Users and Roles.
- You can specify schemas to exclude, and object types. This form of scope specification captures objects that are contained in all schemas other than those you specify. For example, you can capture all object types in schemas other than SYSTEM and SYS. This form of scope specification is appropriate when you want to capture all database objects, with the exception of objects contained in Oracle-provided schemas. As with the first form of scope specification, you can also capture non-schema objects and privilege grants.
- Finally, you can capture individual schema objects by specifying the type, schema and name of each object. This form of scope specification is appropriate when you want to capture a few specific objects, rather than all objects contained within one or more schemas. While capturing individual schema objects, you can also capture non-schema objects and privilege grants.

If you include a non-schema object type, such as User or Role, in a scope specification, all objects of that type are captured. There is no way to capture individual non-schema

objects. [Figure 28–1](#) shows the Schema Baselines:Objects page where the scope can be specified.

Figure 28–1 Baseline Scope Specification in the form Of Schemas And Object Types to Capture



28.2.2 Capturing a Schema Baseline Version

As the final step of defining a baseline, you specify when to capture the first version of the baseline. You can capture the first version immediately, or at a later time (for example, when the database is not being used in active development work). You can also indicate that additional versions of the baseline should be captured at regular intervals without further intervention on your part.

You can also capture a new baseline version at any time by selecting the baseline and specifying "Recapture Now."

Baselines processed after the initial version generally complete substantially faster than the initial version. Only those objects that have changed are captured in the new version. This also means that the storage required for additional baseline versions is only slightly larger than the storage used by the initial version, assuming a small percentage of objects has changed. [Figure 28–2](#) shows the first version of a schema baseline.

Figure 28–2 Schema Baseline

ORACLE Enterprise Manager Cloud Control 12c

Setup Help SYSMAN Log Out

Grid Targets Favorites History Search Target Name

Schema Baselines > Baseline: baseline

Baseline: baseline

Refresh

Source Database: database
Owner: SYSMAN
Description:

> Scope Specification

Versions

Select	Version	Objects	Creation Date	Job Status	DDL
<input type="checkbox"/>	1	109	Jul 19, 2011 11:08:44 PM GMT-07:00	Succeeded	Not Generated

28.2.3 Working With A Schema Baseline Version

Within a single schema baseline version, you can examine individual object attributes, generate DDL for individual objects, and generate DDL for all the objects in the baseline version. You cannot modify object definitions captured in baseline versions, since they are intended to represent the state of objects at a particular point in time.

- Viewing a baseline object displays the object's attributes graphically.
- Selecting a baseline object and specifying "Generate DDL" displays the DDL used to create the object. [Figure 28–3](#) shows the DDL generated for a baseline object.

Figure 28–3 DDL Generated for a Selected Baseline Object

- Selecting a baseline version and specifying "Generate DDL" generates the DDL for all objects in the baseline version. While an effort is made to create objects in the correct order (for example, creating tables before indexes), the resulting DDL cannot necessarily be executed on a database to create the objects in the baseline version. For example, if you capture all the schema objects contained in schema APPL1, then try to execute the baseline version DDL on a database that does not contain User APPL1, the generated DDL will fail to execute.

Baseline versions are also used with other Database Lifecycle Management Pack applications, such as Compare and Synchronize. You can compare a baseline version to a database (or to another baseline version). You can also use a baseline version as the source of object definitions in Synchronize, allowing you to re-create the definitions in another database.

28.2.4 Working With Multiple Schema Baseline Versions

When a baseline contains more than one version, you can examine the differences between the versions.

- To see what has changed between a version and the version that precedes it, select the version and specify "View Changes Since Previous Version." The display shows which objects have changed since the previous version (Figure 28–4), which have been added or removed, and which are unchanged. Selecting an object that has changed displays the differences between the object in the two versions.

Figure 28–4 Viewing Changes Since the Previous Version

ORACLE Enterprise Manager Cloud Control 12c

Setup Help SYSMAN Log Out

Grid Targets Favorites History Search Target Name

Schema Baselines > Baseline: baseline_1 > Changes Since Previous Version: baseline_1[2]

Changes Since Previous Version: baseline_1[2] Return

Previous Version 1
Source Database database
Creation Date Jul 19, 2011 10:57:56 PM GMT-07:00

Objects Change Summary

Unchanged 107 Changed 2 New 0 Removed 0

Objects

Object Type Schema Object Name Go

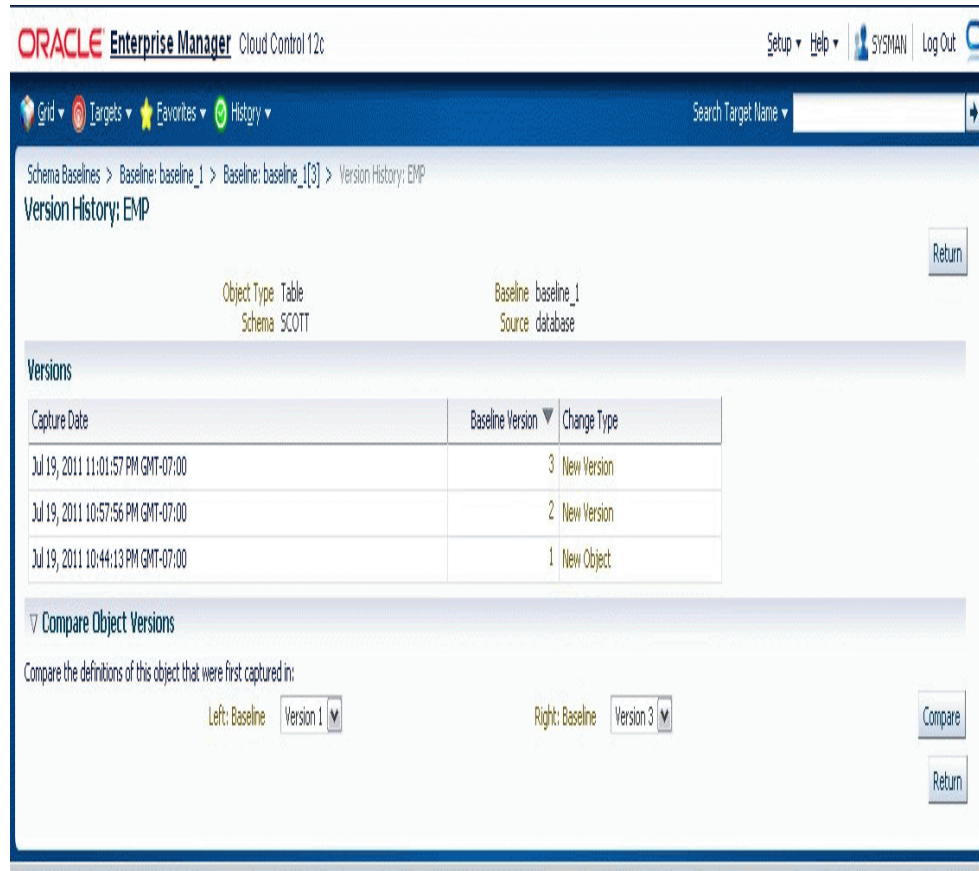
All Types

Show Changed

Schema	Name	Type
SCOTT	DEPT	TABLE
SCOTT	EMP	TABLE

Return

- To see how an individual object has changed over all the versions of the baseline, select the object and specify "View Version History." The display identifies the versions in which the object was initially captured, modified, or dropped as shown in Figure 28–5. From this display, you can compare the definitions of the object in any two baseline versions.

Figure 28–5 Viewing Version History of a Selected Baseline Object

28.2.5 Exporting and Importing Schema Baselines

You can use the export/import baseline functionality for the following:

- Transferring baselines between two Cloud Control sites with different repositories.
- Offline storage of baselines. Baselines can be exported to files, deleted, and then imported back from files.

You can select a schema baseline or a version and then export it to a file. The system uses Data Pump for export and import. The dump files and log files are located in the Cloud Control repository database server host. They can be located in directories set up on NFS file systems, including file systems on NAS devices that are supported by Oracle.

28.2.5.1 Creating Directory Objects for Export and Import

To export a schema baseline version from the repository to an export file or import schema baselines from an import file on the repository database server, select the directory object in the repository database for the export or import and specify a name for the export or import file.

To create a new directory object for export or import, do the following:

1. Log in to the repository database as a user with CREATE ANY DIRECTORY privilege or the DBA role.

2. Create a directory object as the alias for a directory on the repository database server's file system where the baselines are to be exported or where the import dump file is stored.
3. Grant READ and WRITE privileges on the directory object to SYSMAN.

The newly created directory will be available for selection by Cloud Control administrators for export and import of schema baselines. Data pump log files from the export and import operations are also written to the same directory.

During import, new values can be set for name, owner, and source database. Super administrators can set another administrator as the owner at the time of import.

The export operation does not export job information associated with a baseline. On import, the job status will hence be unknown.

For non-super administrators, the following applies:

- Non-super administrators can export their own baselines. They can also export a version of baseline owned by another administrator, provided they have the privilege to view the version and see the list of schema objects in that version.
- At the time of import, a non-super administrator must become the owner of the baseline being imported. A non-super administrator cannot set another administrator as the owner. If the baseline in the import dump file was owned by another administrator, its new owner is set to the logged-in non-super administrator at the time of import.
- View privileges granted on the baseline to non-super administrators are lost during import and cannot be re-granted after the import, since there is no associated job information.

28.3 Overview of Schema Comparisons

A schema comparison identifies differences in database object definitions between a baseline or a database and a baseline or a database, or two schemas within a single database/baseline.

A comparison specification is defined by left and right sources, scope, and owner. The scope specification describes the names and types of database object definitions to be included in the comparison and the schemas that contain these object definitions.

Comparisons identify differences in any attribute value between objects of any type. Use comparisons to create multiple versions of a comparison. Each version has a unique version number and a comparison date. Use these versions to associate comparisons of database/schemas made over time.

Examples:

Comparisons show differences between definitions in the original baseline for your application and those in your current database. After creating a new comparison version, it identifies the differences between the original definitions at the start of the development cycle, and those same definitions at the current time.

Use another comparison specification to compare definitions from your most recent baseline with those in your previous baseline. With each newly created version of this comparison using the comparison specification, that comparison version identifies the differences in the definitions since the previous baseline.

28.3.1 Defining Schema Comparisons

A schema comparison definition consists of left and right sources for metadata definitions, the scope specification, an optional schema map, and comparison options. Once created, a schema comparison definition cannot be modified. This ensures that each version of the schema comparison reflects changes in the databases being compared and not in the comparison's definition.

Schema Comparison Sources

Each comparison has a left source and a right source. The comparison matches object definitions from the left and right sources. A source can be a database or a baseline version.

- When the source is a database, object definitions are taken directly from the database at the time the comparison version is created.
- When the source is a baseline, object definitions are taken from the specified baseline version. Using a baseline version allows you to compare a database (or another baseline version) to the database as it existed at a previous point in time. For example, a baseline version might represent a stable point in the application development cycle, or a previous release of the application.

For baseline sources, there are various ways to specify the version to be used.

- If you want a specific baseline version to be used in all versions of the comparison, specify the baseline version number. This is appropriate for comparing a well-defined previous state of the database, such as a release, to its current state.
- You can also request that the latest or next-to-latest version be used in the comparison. If you specify "Latest," you can also request that the baseline version be captured before the comparison takes place. This option allows you to capture a baseline and compare it to the other source in a single operation. For example, every night, you can capture a baseline version of the current state of a development database and compare it to the previous night's baseline, or to a fixed baseline representing a stable point in development.

Scope Specification

The scope specification for a schema comparison identifies the objects to compare in the left and right sources. Creating a comparison scope specification is the same as creating a baseline scope specification, described in the "Schema Baselines" section. As with baselines, you can specify object types and schemas to compare, or individual objects to compare.

Schema Map

Normally, schema objects in one source are compared to objects in the same schema in the other source. For example, table APPL1.T1 in the left source is compared to APPL1.T1 in the right source.

However, there may be cases where you want to compare objects in one schema to corresponding objects in a different schema. For example, assume that there are two schemas, DEV1 and DEV2, which contain the same set of objects. Different application developers work in DEV1 and DEV2. You can use the optional schema map feature to allow you to compare objects in DEV1 to objects with the same type and name in DEV2.

To add entries to the schema map, expand the "Mapped Objects" section of the comparison "Objects" page. You can create one or more pairs of mapped schemas. Each pair designates a left-side schema and a corresponding right-side schema.

When using a schema map, you can compare objects within a single database or baseline version. In the example above, DEV1 and DEV2 can be in the same database. You specify that database as both the left and right source, and supply the schema map to compare objects in DEV1 to those in DEV2.

Comparison Options

You can select several options to determine how objects are compared. These options allow you to disregard differences that are not significant. The options include the following:

- "Ignore Tablespace" and "Ignore Physical Attributes" – These two options allow you to compare stored objects without regard to the tablespaces in which they are stored or the settings of their storage-related attributes. This is useful when you are comparing objects in databases having different size and storage configurations, and you are not interested in differences related to the storage of the objects.
- "Match Constraints By Definition" or "By Name" — If you are more interested in the definitions of table constraints – for example, the columns involved in primary or unique constraints – choose "Match Constraints By Definition." This causes constraints with the same definitions to match; their names appear as differences (unless you also choose "Ignore Name Differences"). If the names of constraints are meaningful, choose "Match Constraints By Name." With this choice, constraints with the same names will match and their definitions will appear as differences.
- "Partitioned Objects: Ignore Partitioning" — Choose this option to ignore partitioning in tables and indexes.
- "Partitioned Objects: Ignore High Values" — Tables that are otherwise the same might have different partition high values in different environments. Choose this option to ignore differences in high values.
- "Logical SQL Compare" — Choose this option to ignore meaningless formatting differences in source objects such packages, package bodies, procedures and functions and to ignore white space differences in comments.
- "Compare Statistics" — Choose this option to compare optimizer statistics for tables and indexes.
- "Ignore Table Column Position" — Choose this option if tables that differ only in column position should be considered equal.

Creating Comparison Versions

When you have finished defining the comparison, you specify when to create the first comparison version. You can create the first version immediately, or at a later time. You can also schedule new comparison versions at regular intervals.

In addition to scheduling comparison versions, you can create a new comparison version at any time by selecting the comparison and specifying "Repeat Now."

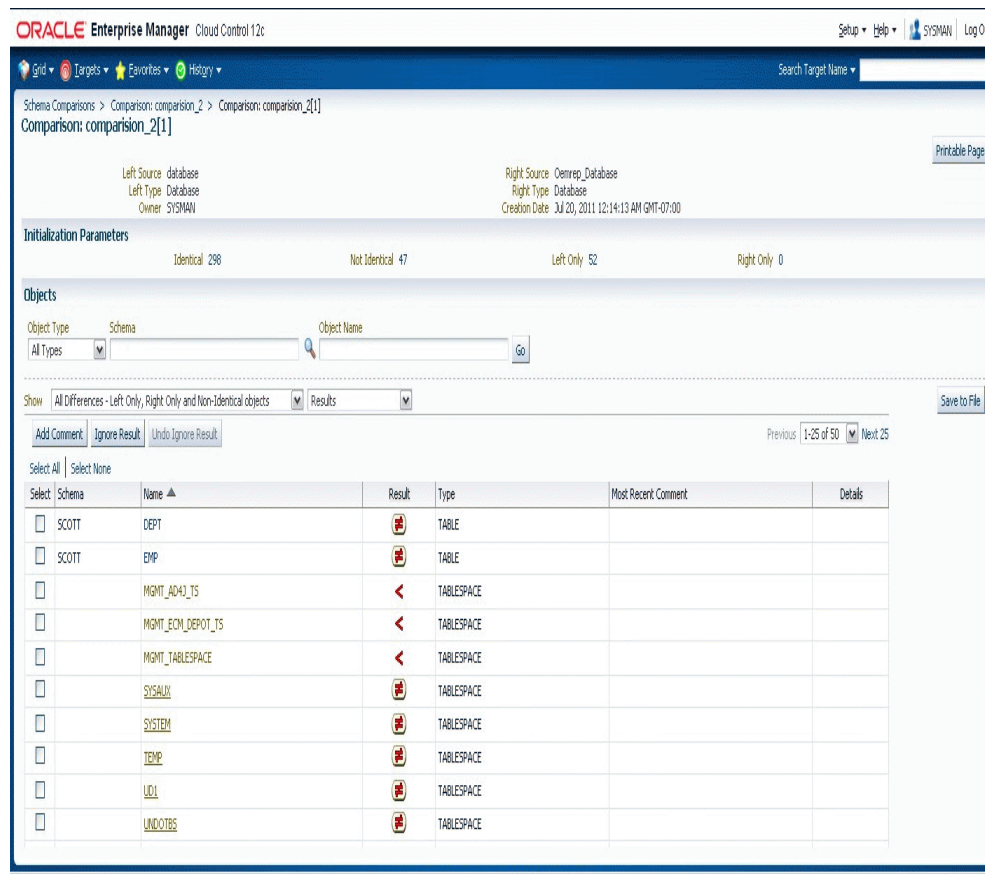
Comparisons processed after the initial version generally complete substantially faster than the initial comparison. Only those objects that have changed on the left or right side are compared in the new version. This also means that the storage required for additional comparison versions is only slightly larger than the storage used by the initial version, assuming a small percentage of objects has changed.

28.3.2 Working with Schema Comparison Versions

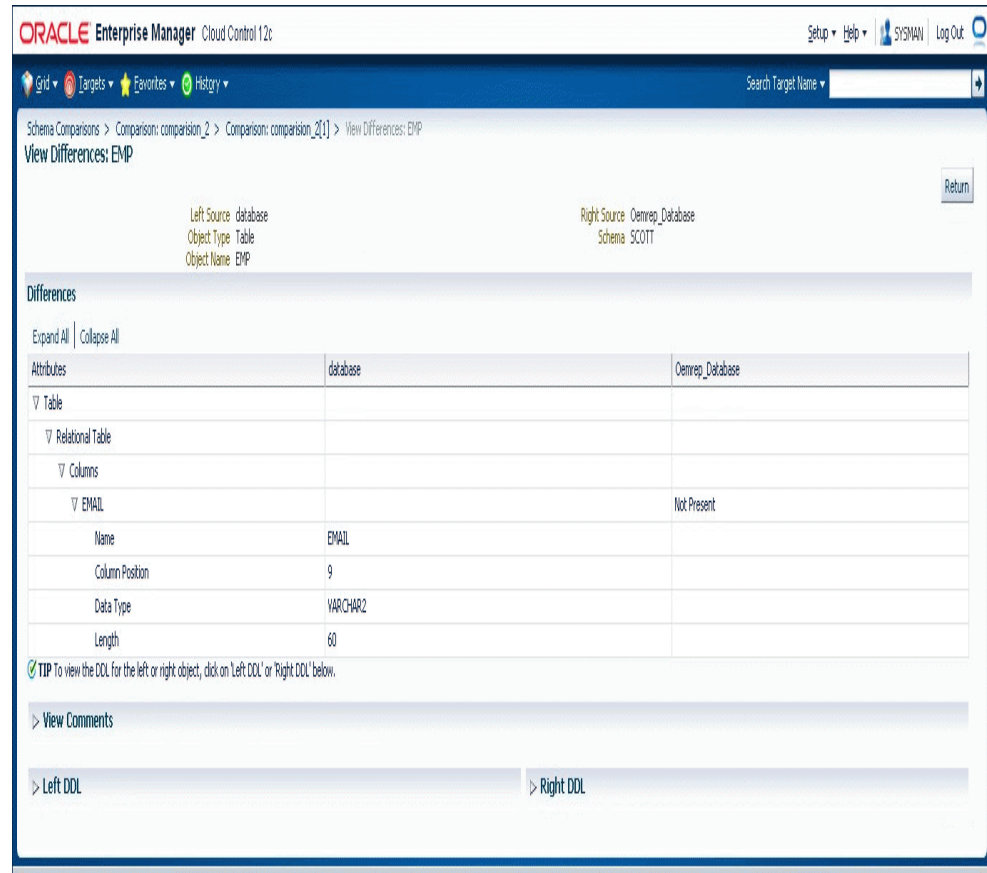
A schema comparison version records the results of comparing the left and right sources in accordance with the scope specification. Objects in a comparison version have one of four states:

- Left Only – The object is present only in the left source.
- Right Only – The object is present only in the right source.
- Identical – The object is present in both left and right sources, and is the same.
- Not Identical – The object is present in both left and right sources, and is different.

Figure 28–6 Comparison Version Page Showing a List Of Not Identical Objects



The page lists all versions of a comparison and shows the number of objects in each state within each version. On the Comparison version page shown in [Figure 28–6](#), you can see the objects in each state individually. Objects that are "Not Identical" can be selected to view the differences, and to generate DDL for the left and right definitions as shown in [Figure 28–7](#).

Figure 28–7 Viewing Differences in the Attributes of a Selected Not Identical Object

You can take two further actions to record information about objects in a comparison version:

- You can add a comment to an object. For example, the comment might explain why two objects are different.
- You can ignore the object. Ignoring the object removes it from lists of comparison version objects. You might ignore an object that is different if you decide that the difference is not important.

28.4 Overview of Schema Synchronizations

A schema synchronization synchronizes differences in database object definitions between two databases or a baseline and a database. The basic action of a database synchronization is to create or modify selected object definitions in a database to match those in another database or in a baseline.

Synchronizations are generated using synchronization specifications. For synchronizations, the scope specification does not include the names of individual objects. It can only specify the types, and the schemas to be included or excluded. You can additionally supply a prefix to limit the objects selected to those whose names start with that prefix.

Schema synchronizations synchronize differences in any attribute value between objects of any supported type. Use synchronization specifications to create multiple versions of a synchronization. Each version has a unique version number and a

synchronization date. Use these versions to associate synchronizations of database/schemas made over time.

28.4.1 Defining Schema Synchronizations

Source and Destination

The synchronization source provides the object definitions (and optionally, the data) from which the destination database is synchronized. A synchronization source may be a database, or a baseline version. If the source is a baseline version, it is not possible to propagate data to the destination, since a baseline does not capture data.

The synchronization destination must always be a database. The purpose of synchronization is to create or modify object definitions in the destination to match those in the source.

The options for specifying which version of a source baseline to use are similar to those used with schema comparisons. You can specify a fixed baseline version, or "Latest" or "Latest-1". If you specify "Latest," you can also request that the baseline version be captured first before synchronizing the destination from it.

When defining a baseline to be used as the source for synchronization, it is important that the baseline contain all the objects to be synchronized. For this reason, the baseline's scope specification should include at least all the schemas and object types that will be synchronized. The baseline should also include User and Role objects, along with privilege grants. A baseline to database synchronization is recommended in environments where changes are expected to be applied to the source database frequently thus necessitating the need for a point-in-time snapshot of the database, i.e. a baseline as the source of the synchronization.

Scope Specification

Defining a scope specification for a schema synchronization is similar to defining a scope specification for a schema baseline or comparison. However, there are restrictions on what you can include in the scope specification.

- You cannot specify individual objects for synchronization. You must specify object types and either schemas to include or schemas to exclude.
- Certain schemas, such as SYS and SYSTEM, cannot be synchronized.
- You cannot directly include User and Role objects for synchronization. (However, Users and Roles are automatically included as needed during the synchronization process.)
- Oracle recommends that the following object types be selected as a group: Table, Index, Cluster, Materialized View, and Materialized View Log.

The scope specification for a synchronization should be carefully tailored to the application. Do not include more schemas than are needed. For example, if you are synchronizing a module of a large application, include only those schemas that make up the module. Do not attempt to synchronize a large application (or the entire database) at one time.

Schema Map

The definition and use of the schema map is the same in schema synchronizations as in schema comparisons. When you use a schema map, object definitions in each schema map are synchronized to the mapped schema in the destination, rather than to the schema with the same name. In addition, schema-qualified references (other than

those contained in PL/SQL blocks and view queries) are changed according to the schema map.

For example, assume the schema map has two entries, as follows:

- DEV1A -> DEV2A
- DEV1B -> DEV2B

Table DEV1A.T1 has an index, DEV1A.T1_IDX. It also has a foreign key constraint that refers to DEV1B.T2. Synchronize will create objects as follows:

- Table DEV2B.T2
- Table DEV2A.T1, with a foreign key reference to table DEV2B.T2
- Index DEV2A.T1_IDX, on table DEV2A.T1

Synchronization Options

Schema synchronization options are similar to the options you can specify with schema comparisons. In synchronization, the options perform two functions:

- During initial comparison of source and destination objects, the options determine whether differences are considered meaningful. For example, if the "Ignore Tablespace" option is selected, tablespace differences are ignored. If two tables are identical except for their tablespaces, no modification to the destination table will occur.
- When generating the script that creates objects at the destination, some options control the content of the script. For example, if "Ignore Tablespace" is selected, no TABLESPACE clauses are generated.

In addition to the options provided with schema comparison, the following options are specific to Synchronize:

- "Preserve Data In Destination" and "Copy Data From Source"—These two options control whether table data is copied from the source database to the destination database. (The option is not available if the source is a baseline.) By default, Synchronize preserves data in destination tables. Choosing "Copy Data From Source" causes Synchronize to replace the destination data with data from the source table.
- "Drop Destination-Only Schema Objects"—Choosing this option directs Synchronize to drop schema objects that are present in the destination but not the source. For example, if the source contains table DEV1.T1 and the destination contains DEV1.T1 and DEV1.T2, Synchronize will drop DEV1.T2 if this option is chosen. This action applies only to schema objects that are within the scope specification. By default, Synchronize does not drop destination-only objects. Synchronize never drops non-schema objects.

Synchronization Mode

The next step in defining a synchronization is to choose the synchronization mode. There are two options:

- Unattended synchronization mode carries out the entire synchronization process in one step, ending with execution of the synchronization script. However, if an error is detected that makes it impossible to generate a correct script, the process will terminate without attempting to execute the script.
- Interactive synchronization mode pauses after initial comparison of the source and destination objects, and again after generation of the synchronization script. Interactive mode gives you a chance to examine the results of comparison and

script generation, and to take appropriate action before proceeding with the next step.

Creating Synchronization Versions

When you have finished defining the synchronization, you specify when to create the first synchronization version. You can create the first version immediately, or at a later time. You can also schedule new synchronization versions at regular intervals.

Depending on the synchronization mode you select, the synchronization may run to completion (unattended mode), or pause after initial object comparison (interactive mode). In the latter case, you run each subsequent phase of the synchronization in a new job.

When using interactive mode, the destination database should not be modified from the time the objects are initially compared until the synchronization script has executed. Otherwise, the script may encounter problems. For example, assume the source has a table that the destination does not have. Object comparison notes the source-only table, and the generated script includes statements to create the table. However, after object comparison but before script execution, you manually create the table at the destination database. The script will fail when it attempts to create the table because the table already exists.

Figure 28–8 shows a list of synchronizations.

Figure 28–8 List of Synchronizations

Select	Name	Source	Destination	Versions	Owner	Most Recent Version	Most Recent Status	Pending Action
<input checked="" type="radio"/>	synch_errors_2	baseline_2(Latest)	database	1	SYSMAN	Jul 20, 2011 1:56:18 AM GMT-07:00	Generated With Errors	Regenerate Script
<input type="radio"/>	synch_errors	baseline_2(Latest)	database	1	SYSMAN	Jul 20, 2011 1:41:25 AM GMT-07:00	Version Abandoned	
<input type="radio"/>	synch_from_baseline	baseline(Latest)	database	1	SYSMAN	Jul 20, 2011 12:52:20 AM GMT-07:00	Comparison Succeeded	Generate Script
<input type="radio"/>	synch_straight_through	Oranrep_Database	database	1	SYSMAN	Jul 20, 2011 12:47:37 AM GMT-07:00	Execution Succeeded	
<input type="radio"/>	synch_2	Oranrep_Database	database	1	SYSMAN	Jul 20, 2011 12:39:41 AM GMT-07:00	Generated With Warnings	Execute Script or Regenerate Script
<input type="radio"/>	synch_1	Oranrep_Database	database	2	SYSMAN	Jul 20, 2011 12:32:32 AM GMT-07:00	Generation Succeeded	Execute Script or Regenerate Script

Related Links
[Schema Baselines](#) [Schema Comparisons](#) [Schema Change Plans](#)

For more information about the process of synchronization, see [Working with Schema Comparison Versions](#).

28.4.2 Creating a Synchronization Definition from a Comparison

You can use a schema comparison as the starting point for synchronization. Select the comparison, then choose "Synchronize." This creates a new synchronization with the following initial information from the comparison:

- Source and destination, from the comparison's left and right sources, respectively. This means that you cannot create a synchronization from a comparison whose right source is a baseline.
- Scope specification. Note that some comparison scope specification options are not available in a synchronization. For example, you cannot synchronize individual schema objects, User objects, or Role objects.
- Comparison options

28.4.3 Working with Schema Synchronization Versions

Each synchronization version represents an attempt to modify the destination objects selected by the scope specification to match the corresponding source objects. (It is "an attempt" because the process may not complete, for various reasons.) This section describes how a schema synchronization version is processed, and how you can monitor and control the process.

28.4.3.1 The Schema Synchronization Cycle

There are three steps involved in processing a synchronization version. As noted previously, you can combine these steps into one (by choosing "Unattended Mode") or run each step separately (by choosing "Interactive Mode"). In either case, all three steps must be carried out when processing a successful synchronization version.

The following sections detail each of the three steps and describe what you can do following each step, when operating in interactive mode.

Object Comparison Step

The first step is to compare objects in the source to corresponding objects in the destination. Only those objects selected by the scope specification are compared. At the end of this step, the synchronization version has recorded all the objects. Each object is in one of the following states:

- Source Only
- Destination Only
- Identical
- Not Identical

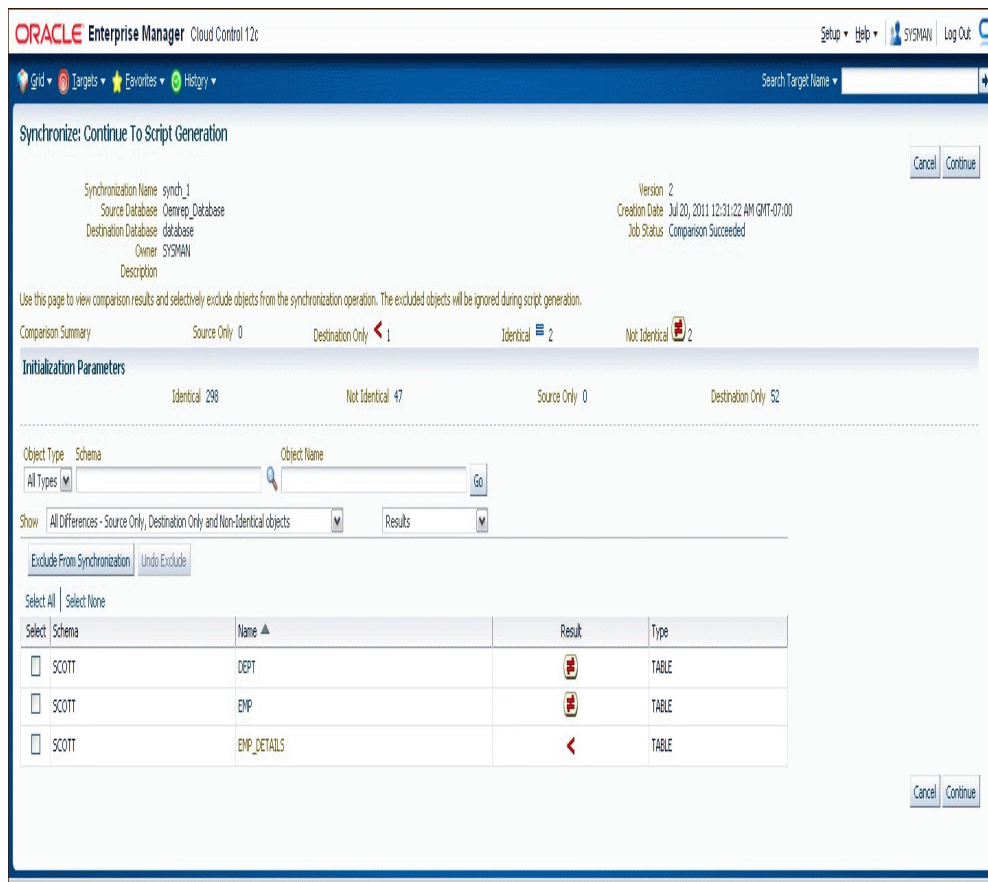
In interactive mode, you can view the objects that are in each state, or all objects at once. For objects that are not identical, you can view the differences between the objects. At this stage, you can anticipate what will happen to each destination object:

- Source-only objects will be created in the destination.
- Destination-only objects will be unaffected, unless you chose the "Drop Destination-Only Schema Objects" option, in which case they will be dropped from the destination.

- Identical objects will be unaffected. However, if you chose the "Copy Data From Source" option, the data in tables that are identical will be replaced with data from the source.
- Non-identical objects will be modified to match the source object. Depending on the differences, the modification may be done with ALTER statements or by dropping and re-creating the object.

Before proceeding to script generation (Figure 28–9), you can exclude objects from the synchronization. For example, if you notice a source-only view that you do not want to create at the destination, you can exclude it now.

Figure 28–9 Continue to Script Generation Step in the Interactive Mode



Script Generation Step

During script generation, Synchronize uses the results of the comparison step to create the PL/SQL script that will create and modify objects at the destination so that it matches the source. As part of script generation, several activities take place:

- Dependency analysis assures that the destination database provides a suitable environment for each object and that objects are created and modified in the correct order.
- Change analysis determines whether an object can be modified with ALTER statements or if it must be dropped and re-created.

- Messages are placed in the impact report for the synchronization version. The messages provide information about the synchronization process, and may report one or more error conditions that make it impossible to generate a usable script.
- The DDL statements needed to carry out the synchronization are generated and recorded in the synchronization version.

Dependency analysis examines each object to determine its relationships with other objects. It makes sure these other objects exist (or will be created) in the destination. Some examples of these relationships are:

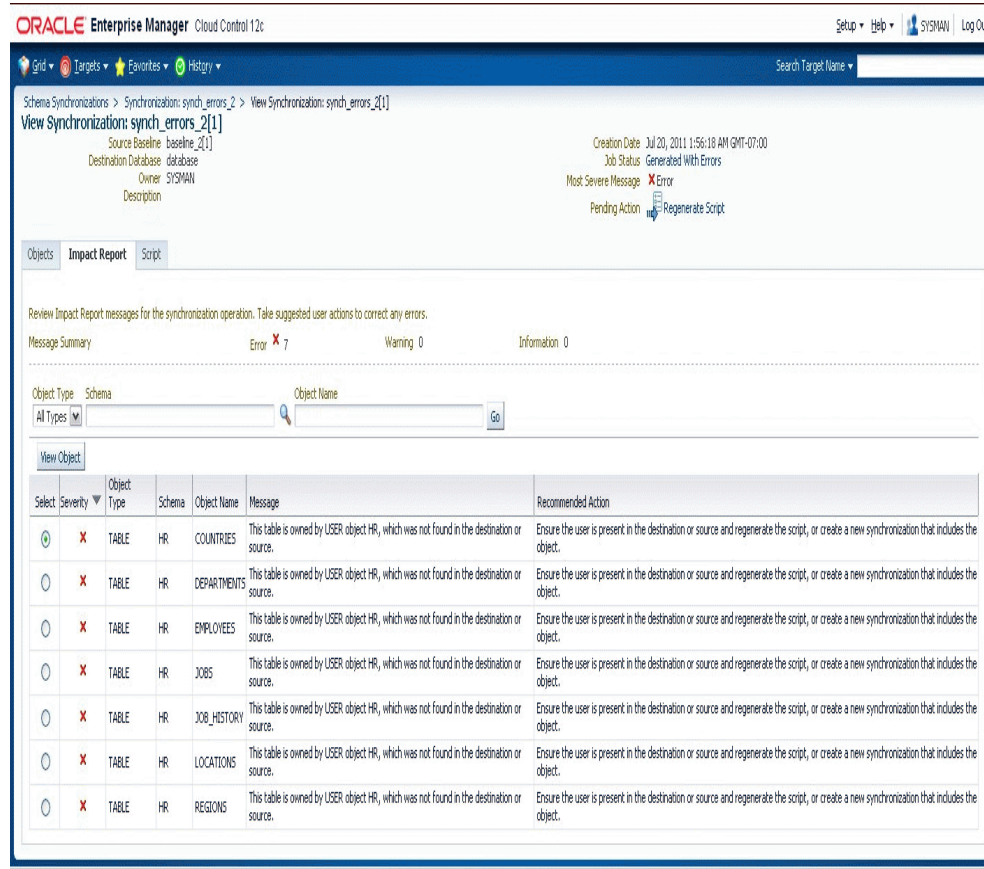
- A schema object depends on the User object that owns it. For example, table DEV1.T1 depends on user DEV1.
- An index depends on the table that it is on. For example, index DEV1.T1_IDX depends on table DEV1.T1.
- A table that has a foreign key constraint depends on the table to which the constraint refers.
- A source object such as a package body depends on other source objects, tables, views, and so on.
- A stored object depends on the tablespace in which it is stored, unless you choose "Ignore Tablespace."

The relationships established during dependency analysis are used later in the script generation process to make sure script statements are in the correct order.

Dependency analysis may determine that a required object does not exist in the destination database. For example, a schema object's owner may not exist in the destination database. Or, a table may have a foreign key constraint on another table that is in a different schema. There are several possible outcomes.

- If the required object is in the source and is selected by the scope specification, Synchronize creates the object. For example, if DEV1.T1 has a foreign key constraint that refers to DEV2.T2, and both DEV1 and DEV2 are in the scope specification, Synchronize creates DEV2.T2.
- If the required object is a user or role, and the object is available in the source, Synchronize automatically includes the user or role and creates it at the destination. This occurs even though User and Role objects are not part of the Synchronize scope specification.
- If a required schema object is in the source but is not selected by the scope specification, Synchronize does not automatically include the object; instead, it places an Error-level message in the impact report. This restriction prevents uncontrolled synchronization of objects outside the scope specification. It is for this reason that scope specifications should include all the schemas that make up the application or module.
- If the source is a baseline version, it may not include the required object. For example, a baseline might not capture Users and Roles. Synchronize cannot look for objects outside the baseline version, so it places an Error-level message in the impact report as shown in [Figure 28–10](#). This is why it is important to include Users, Roles, and privilege grants in any baseline that will be used for synchronization.

Figure 28–10 Error-level Impact Report Messages Resulting from a Required Schema Object Not Selected by the Scope Specification



At the end of the script generation step, Synchronize has added the impact report and the script to the synchronization version. In interactive mode, you can examine the script and impact report before proceeding to script execution.

The impact report contains messages about situations that were encountered during script generation. There are three types of messages:

- Informational messages require no action on your part. They simply report something of interest. For example, when script generation automatically includes a User object, it adds an informational message to the impact report.
- Warning messages report a situation that requires your attention, but that may not require action. For example, if Synchronize is unable to determine if a reference in a source object can be resolved, it adds a warning message to the impact report. You need to verify that situations reported in warning messages will not prevent script execution.
- Error messages indicate a situation that will prevent script execution if not corrected. For example, if Synchronize is unable to locate a required dependency object, it adds an error message to the impact report. Depending on the message, you may be required to create a new synchronization. For example, if the dependency object is not in the synchronization scope, or if the source is a baseline that does not contain the dependency object, you will need to create a new synchronization with an expanded scope or a different source baseline. In other

cases, you can resolve the situation by excluding one or more objects from the synchronization and regenerating the script.

The script display contains the statements of the generated script in the order they will be executed. You can examine the script if you have any concerns about its correctness. The display allows you to locate statements that are associated with a particular object or object type.

Figure 28–11 Continuing To Script Execution Step in the Interactive Mode (Impact Report Tab)

ORACLE Enterprise Manager Cloud Control 12c

Synchronize: Continue To Script Execution

Synchronization Name: synch_2
 Source Database: Oemrep_Database
 Destination Database: database
 Owner: SYSMAN
 Description:

Version 1
 Creation Date: Jul 20, 2011 12:37:00 AM GMT-07:00
 Job Status: Generated With Warnings
 Most Severe Message: Warning

Impact Report | Script

Review Impact Report messages for the synchronization operation. Take suggested user actions to correct any errors.

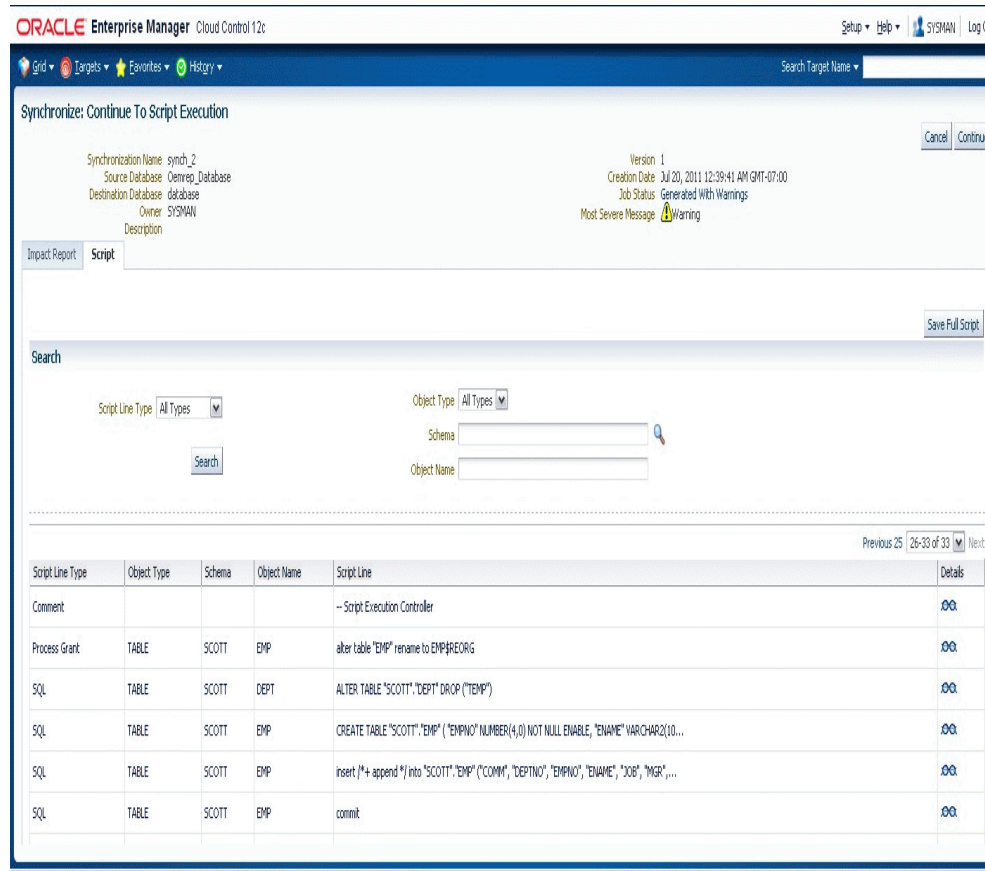
Message Summary: Error 0, Warning 9, Information 0

Object Type: Schema, Object Name: [Search] Go

Severity	Object Type	Schema	Object Name	Message	Recommended Action
Warning				Initialization parameter control_files is not dynamic. This change will not take effect until the database is restarted.	Restart the database after synchronization.
Warning				Initialization parameter db_domain is not dynamic. This change will not take effect until the database is restarted.	Restart the database after synchronization.
Warning				Initialization parameter db_name is not dynamic. This change will not take effect until the database is restarted.	Restart the database after synchronization.
Warning				Initialization parameter db_unique_name is not dynamic. This change will not take effect until the database is restarted.	Restart the database after synchronization.
Warning				Initialization parameter diu_locks is not dynamic. This change will not take effect until the database is restarted.	Restart the database after synchronization.
Warning				Initialization parameter event is not dynamic. This change will not take effect until the database is restarted.	Restart the database after synchronization.
Warning				Initialization parameter instance_name is not dynamic. This change will not take effect until the database is restarted.	Restart the database after synchronization.
Warning				Initialization parameter instance_number is not dynamic. This change will not take effect until the database is restarted.	Restart the database after synchronization.
Warning				Initialization parameter log_archive_format is not dynamic. This change will not take effect until the database is restarted.	Restart the database after synchronization.

Following script generation, you can continue to script execution unless an error was encountered during the script generation step (Figure 28–11 and Figure 28–12). In this case the impact report will contain one or more Error-level messages detailing the problem and solution. In some cases, you may be able to solve the problem by selecting "Regenerate Script," excluding an object from the synchronization, and regenerating the script.

Figure 28–12 Continuing To Script Execution Step in the Interactive Mode (Script Tab)



There may be cases where you need to create a new version of the synchronization in order to correct the problem. For example, if you need to modify the definition of an object in the source or destination or add an object in the destination, you will need to create a new version. This allows the new or modified object to be detected during the comparison step. In this case, the old version becomes "abandoned" since you cannot continue to script generation.

Script Execution Step

Following successful script generation, the script is ready to execute. In unattended mode, the script executes as soon as script generation completes. In interactive mode, you proceed to script execution as soon as you have reviewed the impact report and the script.

The script executes in the Cloud Control job system. [Figure 28–13](#) shows the output of the Synchronization job. Once script execution is complete, you can view the execution log. If the script fails to execute successfully, you may be able to correct the problem and re-start the script execution from the point of failure. For example, if the script fails due to lack of space in a tablespace, you can increase the size of the tablespace, then re-start the script.

Figure 28–13 Synchronization Script Execution Step Output of Cloud Control Job

```

ORACLE Enterprise Manager Cloud Control 12c
Setup Help SYSMAN Log On
Grid Targets Favorites History Search Target Name
Job Activity > Execution: 2 > Step: SynchScriptExecution
Step: Synchronization Script Execution
Page Refreshed Jul 20, 2011 12:58:02 AM PDT
View Data Manual Refresh
Status Succeeded Started Jul 20, 2011 12:47:49 AM GMT-07:00
Exit Code 0 Ended Jul 20, 2011 12:47:56 AM GMT-07:00
Step ID 1407 Step Elapsed Time 7 seconds
Targets database Management Service adcs6140459.us.oracle.com:17707_Management_Service
TIP Management Service from which the job step was dispatched.

Output Log

SQL*Plus: Release 11.2.0.2.0 Production on Wed Jul 20 00:47:51 2011

Copyright (c) 1982, 2010, Oracle. All rights reserved.

SQL> Connected.
SQL> -- Script Execution Controller
Starting Synchronization
USER is 'SYSTEM'
No open DBLink.
Database link not found.
Database link created.
DROP TABLE 'SCOTT'. 'DEPT' PURGE
DROP TABLE 'SCOTT'. 'SALGRADE' PURGE
DROP TABLE 'SCOTT'. 'EMP' PURGE
DROP TABLE 'SCOTT'. 'BONUS' PURGE
CREATE TABLE 'SCOTT'. 'DEPT'
(
  'DEPTNO' NUMBER(2,0) NOT NULL ENABLE,
  'DNAME'
  VARCHAR2(14),
  'LOC' VARCHAR2(13)
)
insert /*+ append */ into 'SCOTT'. 'DEPT' ('DEPTNO', 'DNAME', 'LOC') select
'DEPTNO', 'DNAME', 'LOC' from 'SCOTT'. 'DEPT'@STNCH#R2ORG
commit
BEGIN
DEMS_STATS.SET_TABLE_STATS(OWNNAME=>'SCOTT', TABNAME=>'DEPT',

```

28.4.4 Creating Additional Synchronization Versions

Following processing of the initial synchronization version, you can create additional versions of the synchronization. Select the synchronization, then choose "Synchronize Again." Note that you cannot choose a different source or destination, or modify the scope specification or synchronization options, when creating a new synchronization version. However, you can choose a different mode (Unattended or Interactive) when starting a new synchronization version.

Creating additional synchronization versions allows you to propagate incremental changes in the source to the destination. For example, you can refresh a test database from the latest changes made to a development system.

Synchronizations processed after the initial version generally complete substantially faster than the initial synchronization.

28.5 Overview of Change Plans

Change Plans are a new feature of the Cloud Control Database Lifecycle Management Pack. Change Plans complement and extend the capabilities of existing Change Management components by allowing users to select and package metadata changes for deployment to multiple databases. Change Plans support database application development methodologies that are not adequately supported by existing Database Lifecycle Management Pack tools such as Schema Synchronizations.

Change Plans are flexible enough to support a variety of development methodologies, yet powerful enough to automate many database administration tasks previously carried out with custom scripts. These tasks include:

- Deploying project-specific development changes from a shared development database to one or more destination databases such as integration, test, or production staging.
- Deploying development changes from a stand-alone project development database to an integration database that collects changes from multiple development databases.
- Upgrading common modules in development databases from a central integration database.

Change Plans are tightly integrated with the other tools in the Database Lifecycle Management Pack. Specifically:

- Change Plan change requests that create objects can get the object definitions from Change Management Schema Baselines.
- Change requests that modify objects can use the contents of an object in a Change Management Schema Comparison to specify the change.
- Change Plans complement Change Management Schema Synchronizations, allowing for finer control of changes and “change-only” change requests.

28.5.1 Working with Change Plans

The first phase of using a change plan to create or modify object definitions is to plan and define the changes that you want to make. For example, you may want to make one or more changes to an existing object definition in one or more databases. Or, you may want to reproduce one or more object definitions from one schema or database in another schema or database.

Figure 28–14 Steps in a Change Plan

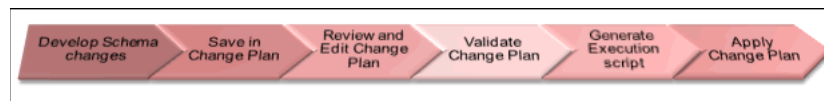


Figure 28–14 shows the steps in a change plan. A change plan is a named container for change requests. You can define change requests to reproduce or modify object definitions at a destination database. A destination database is a database where you want to apply the change requests in a change plan. After you finish planning and defining the changes, evaluate the impact of the changes that you want to make.

To evaluate the impact of the change requests at a particular database, generate a script and an impact report for a change plan and that destination database. The impact report explains the changes that will be made by the script when it executes at the destination database. It also describes any change requests that cannot be applied at the destination database.

To implement the change requests in a change plan at a destination database, execute the script at the destination database.

28.5.2 Creating a Change Plan

This section explains the different methods of creating change plans.

You can create change plans through any of the following ways:

- [Creating and Applying a Change Plan From a Schema Comparison](#)
- [Using External Clients to Create and Access Change Plans in Cloud Control](#)

28.5.2.1 Creating and Applying a Change Plan From a Schema Comparison

This section explains how to create a change plan from a schema comparison.

28.5.2.1.1 Prerequisites to Creating a Change Plan

Following are the prerequisites:

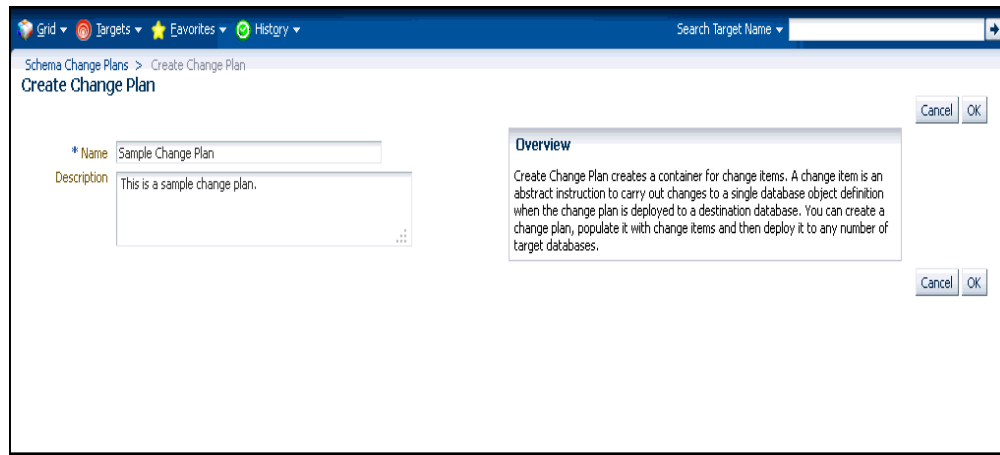
- Ensure that the Application Developer (AD) is an Cloud Control user who has the following privileges:
 - Connect Target privilege to the development and production-staging databases targets or Connect Any Target privilege
 - DBA privileges to the development database
 - Create Privileges for Job System (Resource Privilege)
 - Create new Named Credential (Resource Privilege)
 - Edit Resource Privilege on the change plans
 - Execute Command Anywhere (Target Privilege)
 - EM_ALL_OPERATOR privilege
- Ensure that the Database Administrator (DBA) is an Cloud Control user who has the following privileges:
 - Connect Target privilege to the development and production-staging databases targets or Connect Any Target privilege
 - DBA privileges to the development database
 - Create Privileges for Job System (Resource Privilege)
 - Create new Named Credential (Resource Privilege)
 - Manage Change Plans (Resource Privilege)
 - Execute Command Anywhere (Target Privilege)
 - EM_ALL_OPERATOR privilege
- It is recommended that the development and destination databases are identical at the start of the development work. For example, they may both be at the current production version, or both updated to a common interim development version.
- The Application Developer would have made changes in the development database. After creating a change plan, the application developer can create and update change items in the change plan through external clients such as SQL Developer. For more information, see [Using External Clients to Create and Access Change Plans in Cloud Control](#).

28.5.2.1.2 Creating a Change Plan

Follow these steps:

- Log in to Cloud Control as a database administrator (DBA).
- Identify the schemas that contain application objects.

- Use Metadata Baselines wizard to define a baseline that includes the schemas of interest. Schedule a job to capture the first version of the baseline.
- Save the baseline.
- Use Schema Comparisons wizard to define a comparison between the baseline version and the development database.
- Schedule a job to create the first version of the comparison and save the comparison.
- In the Schema Change Plans page, click **Create**.
- Specify a **Name** and **Description** for the change plan and click **OK** to save the change plan.



- In the Change Items page, click **Create From Comparison**.
- In the Create Change Items from Schema Comparison page, select the Comparison Version created earlier, specify the development database as the Change To side and the production-staging database as the Change From side in the Conversion Assignment and click **OK**.



- In the Create Change Items from Schema Comparison: Select Differences page, select:

- All Differences in the Schema Comparison to add all differences in the comparison to the change plan
- Specific Differences in the Schema Comparison to select the differences in the comparison you want to add to the change plan. Select the differences.

Click **Finish**.

- Submit request to apply the Change Plan on the destination database.

28.5.2.1.3 Applying a Change Plan

Follow these steps:

1. Log in to Cloud Control as a database administrator (DBA).
2. In the DBA role, examine the Change Plan, evaluating its suitability for application to the proposed database. Remove individual Change requests if required.
3. From the Schema Change Plans page, select **Create Synchronization from Change Plan**.
4. Specify the details in the Schema Synchronization wizard with the source as the Change Plan instance created earlier. For information about using the Schema Synchronization wizard, see *Synchronizing with Production Staging*. By default, the synchronization created from change works in the interactive mode.
5. Schedule script generation.
6. Check Impact Report and schedule script execution.
7. Check completed script execution job for errors. If the change plan job failed, do the following:
 - If the failure is due to a condition noted in an impact report error warning, perform the suggested user action.
 - If the failure is due to a condition in the source or destination database that can be fixed manually, fix the problem and perform the operation again.
 - If the failure is in the script execution phase, view the script output in the job details. If the problem can be resolved by actions such as issuing missing grants, fix the problem manually in the database and then click **Retry Script Execution**.
8. Fix the errors and submit the change plan creation job again.

28.5.2.2 Using External Clients to Create and Access Change Plans in Cloud Control

Cloud Control provides support for external clients such as SQL Developer to create and access change plans. You can use these applications to connect to the Cloud Control repository and create change plans and add and update change items in them.

Client users are of two types:

- Users who can create and access all change plans
- Users who can access (view and possibly edit) specific change plans

Following are the steps:

1. Configure the repository database listener to allow access by a trusted client. It is recommended that you make the repository database inaccessible to login from non-trusted clients. For information about configuring the listener, see *Oracle® Database Net Services Administrator's Guide 11g Release 2 (11.2)*.

2. Set up an Cloud Control administrator for use by an external client.

The following section describes how to set up administrators for change plans, for access from Cloud Control and from external clients.

28.5.2.2.1 Setting Up Cloud Control Administrator For Change Plans

Follow these steps:

1. Log in to Cloud Control as a super administrator.
2. From the **Setup** menu, click **Security** and then select **Administrators**.
3. In the Administrators page, click **Create**.
4. In the Create Administrator: Properties page, specify the Name and Password for the user. This creates a database user with the specified name and password, as well as creating the Cloud Control administrator. Click **Next**.
5. In the Create Administrator: Roles page, click **Next**.
6. In the Create Administrator: Target Privileges page, click **Next**.
7. In the Create Administrator: Resource Privileges page, select Change Plan Security Class and click the **Manage Privilege Grants** icon.
8. In the Create Administrator: Manage Privileges page, do the following:
 - If you want to create an administrator who has all access to all change plans, select **Manage Change Plans** in the Resource Type Privileges section.
 - If you want to create an administrator who has specific access to one or more change plans, click **Add** in the Resource Privileges section. In the list of change plans that have been created already, select one or more and click **Select**. The selected plans are added to the Resource Privileges section. By default, the administrator is granted View Change Plan privilege; you can edit this to grant Edit Change Plan privilege.
9. Click **Continue**.
10. In the Create Administrator: Review page, click **Finish** to create the new administrator.
11. For an external client to be able to access change plans using any of these privilege types, follow these steps:
 - a. Log in to the repository database as a user with DBA privileges.
 - b. Grant the **CHANGE_PLAN_USER** database role to the database user corresponding to the new administrator (through Schema->Users in Enterprise Manager Administrator, or in SQL Plus).

28.5.3 Submitting Schema Change Plans From SQL Developer Interface

To enable developers to submit their schema changes to Enterprise Manager Schema Change Plans through SQL Developer interface, perform the following manual configuration steps:

1. Ensure that the repository administrator has configured the repository database to accept remote database connection from SQL developer. You can do this by configuring the repository listener process.
2. Create a local administrator account on the OMS.

3. Provide the repository user of the local OMS account privileges to be a change plan user by running the following SQL commands on the repository database as user SYS:

```
grant CHANGE_PLAN_USER to PUBLIC;
```

or:

```
grant CHANGE_PLAN_USER to <repos_user>;
```

4. Edit the OMS users resource privileges to give the user access to edit the change plans.

28.6 Overview of Data Comparison

A data comparison operation compares data in a set of database objects in a candidate database with those in a reference database. To compare objects residing in the same database, select that database as both the reference and the candidate. You can create a comparison specifying which objects are to be compared and submit a Cloud Control job to compare them immediately or at a later time. On job completion, select the data comparison and view results. The results will be purged when you delete the comparison.

Cloud Control data comparison uses DBMS_COMPARISON package for comparison. It can compare the following types of database objects:

- Tables
- Single-table views
- Materialized views
- Synonyms for tables, single-table views, and materialized views

Database objects of different types can be compared at different databases. For example, a table at one database and a materialized view at another database can be compared.

28.6.1 Requirements for Data Comparisons

For data comparison, you will need to meet the requirements explained in this section.

The database character sets must be the same for the databases that contain the database objects being compared.

For index column, the number, timestamp, and interval columns datatypes are as follows:

- Number columns are of the following datatypes: NUMBER, FLOAT, BINARY_FLOAT, and BINARY_DOUBLE.
- Timestamp columns are of the following datatypes: TIMESTAMP, TIMESTAMP WITH TIME ZONE, and TIMESTAMP WITH LOCAL TIME ZONE
- Interval columns are of the following datatypes: INTERVAL YEAR TO MONTH and INTERVAL DAY TO SECOND.

The database objects must have one of the following types of indexes:

- A single-column index on a number, timestamp, interval, DATE, VARCHAR2, or CHAR datatype column

- A composite index that only includes number, timestamp, interval, DATE, VARCHAR2, or CHAR columns. Each column in the composite index must either have a NOT NULL constraint or must be part of the primary key.

If the database objects do not have one of these types of indexes, then the EM data comparison does not support the database objects. For example, if the database objects only have a single index on an NVARCHAR2 column, then the data comparison does not support them. Or, if the database objects have only one index, and it is a composite index that includes a NUMBER column and an NCHAR column, then the data comparison does not support them.

The index columns in a comparison must uniquely identify every row involved in a comparison. The following constraints satisfy this requirement:

- A primary key constraint
- A unique constraint on one or more non-NULL columns.

If you specify an index, then make sure the columns in the index meet these requirements for comparison.

Data Comparison feature in Cloud Control can compare data in columns of the following datatypes:

- VARCHAR2
- NVARCHAR2
- NUMBER
- FLOAT
- DATE
- BINARY_FLOAT
- BINARY_DOUBLE
- TIMESTAMP
- TIMESTAMP WITH TIME ZONE
- TIMESTAMP WITH LOCAL TIME ZONE
- INTERVAL YEAR TO MONTH
- INTERVAL DAY TO SECOND
- RAW
- CHAR
- NCHAR

If a column with datatype `TIMESTAMP WITH LOCAL TIME ZONE` is compared, then the two databases must use the same time zone. Also, if a column with datatype `NVARCHAR2` or `NCHAR` is compared, then the two databases must use the same national character set.

Data comparison feature cannot compare data in columns of the following datatypes:

- LONG
- LONG RAW
- ROWID
- UROWID

- CLOB
- NCLOB
- BLOB
- BFILE
- User-defined types (including object types, REFs, varrays, and nested tables)
- Oracle-supplied types (including any types, XML types, spatial types, and media types)

You can compare database objects that contain unsupported columns by excluding the unsupported columns when providing comparison specification. Edit the comparison item and include only the supported columns in the Columns To Include list of column names.

Since data comparison cannot compare LOB column values directly, their cryptographic hashes will instead be used for comparison. If you include LOB type columns to be compared, make sure that the database users connecting to the reference and candidate databases have EXECUTE privilege on SYS.DBMS_CCRYPTO package. For more information about DBMS_COMPARISON, see *Oracle Database PL/SQL Packages and Types Reference* for the database version of your reference database

28.6.2 Comparing Data and Viewing Results

The following procedure enables you to specify which pairs of objects you want to compare in the reference and candidate databases, submit a job to process your choices, then view the differences after the job successfully completes.

1. From the main Data Comparisons page, click **Create**. The Create Data Comparison page appears (Figure 28–15).

Figure 28–15 Create Data Comparison Page

2. Provide the required input:
 - a. If you want to compare objects residing in two databases, select one database as the Reference and the other as the Candidate.
 - The Reference database always executes the comparison, so it must be version 11g or later. The Candidate database must be version 10g or later.

- Be advised that the Reference database carries an additional processing load and requires some space to store the row IDs of differing rows (not the entire rows themselves). If you compare data between a production system and a test system, it might be appropriate to process and store the results on the test system.

- b. Click **OK** when you have finished. The Data Comparison Specification page appears.

Tip: It is recommended that you define the comparison specification once and run it many times.

- 3. Open the **Actions** menu, then select **Add Object Pair** or **Add Multiple Objects**. If you select Object Pair, continue with the following sub-steps. If you select Multiple Objects, go to step 4.

- a. Specify the reference and candidate objects. The reference database can be the same as the candidate database. In this case, the objects are from the same database.
- b. Select one or more columns in the reference or candidate databases for comparison. The columns included must be common to both objects.
- c. Optionally select an index to be used for comparison. Columns in the comparison index must uniquely identify every row involved in a comparison. An index used for a primary key constraint or a unique constraint on one or more non-NULL columns satisfies this requirement. The comparison can use the specified index only if you select all of the columns in the list of Columns To Include.

You can select a composite index if you want to add multiple index columns.

- d. Specify an optional Where Condition per pair of objects being compared.
- e. Either specify or let the system compute the maximum number of buckets and minimum rows per bucket.

See Also: ["Usage of Buckets"](#) below.

- f. Specify the point in time you want to compare data.

* The System Change Number (SCN) is a sequential counter that uniquely identifies a precise moment in the database. This is the most accurate way to identify a moment in time. Whenever you commit a transaction, Oracle records a new SCN. You can obtain SCNs from the alert log.

- g. When you have finished the configuration, click **OK**.

The Data Comparison Specification page reappears, showing your selected objects in the list.

- h. Click **OK**, then go to step 5.

- 4. Open the **Actions** menu, then select **Add Multiple Objects**.

- Adding multiple objects enables you to conveniently perform a bulk inclusion of multiple objects from the reference database into the specification. You can search and select multiple objects, such as many tables and views, from the reference database list of values, and then edit each item as needed.

- a. Specify the schema name, one or more object types, then click **Search**.

The table populates with object names.

- b. Select the objects you want to compare, then click **OK**.

The Data Comparison Specification page reappears, showing your selected objects in the list.

5. Select your comparison name from the list, open the **Actions** menu, then select **Submit Comparison Job**. For information about privileges required for user credentials for the reference and candidate databases, see [Overview of Change Management for Databases](#).

6. Provide the required credentials in the page, schedule the job, then click **OK**.

The Data Comparisons page reappears and displays the following confirmation message:

"The job was submitted successfully. Click the link in the Job Status column to view job status."

After the Job Status column shows Succeeded, go to the next step.

7. Select your comparison name from the list, open the **Actions** menu, then select **View Results**. The Data Comparison Results page appears.

8. Look for rows in the Result column with the **≠** symbol, indicating that there are differences between reference row and candidate row data.

- Data comparison attempts to compare all tables. If there is an error, you can see the error message by selecting the **Messages** tab. An error message is indicated with an X instead of the = or ≠ symbol.

- You can see the SQL statements that are running to perform the comparison by clicking the **Executed Statements** tab.

9. Select a dissimilar Reference/Candidate row, then click **View Row Differences** to see a detailed, indexed list of reference-only, candidate-only, and non-identical changed rows on the Row Data Differences page ([Figure 28-16](#)).

- The Row Source column indicates the origin of each row of data as a whole. Furthermore, data in a row differing between reference and candidate are displayed in contrasting colors, indicating whether the source of the data is the reference or candidate database.

- The comparison is shown based on a key column (depending on a chosen unique index). If the key column value is different, the row appears as a candidate or reference-only row. If other columns are different, the row appears as a non-identical row.

Figure 28–16 Row Data Differences Page

ORACLE Enterprise Manager Cloud Control 12c

Setup Help SYSTEM Log Out

Enterprise Targets Favorites History Search Target Name

Row Data Differences: HR data comparison Page Refreshed Aug 9, 2011 1:39:31 AM PDT Return

Reference Database: database3 Candidate Database: database_2
 Logged in As: SYSTEM Logged in As: SYSTEM
 Reference Object: "HR"."EMPLOYEES" Candidate Object: "HR"."EMPLOYEES"
 Index Columns: EMPLOYEE_ID

Rows are categorized based on their index column values. Reference only and candidate only rows are those with index column values that exist only in reference and candidate respectively. Non-identical rows are those with index column values present on both sides, but with one or more differences in the other (non-index) column values.

Show Reference Only Rows Candidate Only Rows Non-identical Rows

View Export To Excel

Row Source	EMPLOYEE_ID	COMMISSION_PCT	DEPARTMENT_ID	EMAIL	FIRST_NAME	HIRE_DATE	JOB_ID	LAST_NAME	MANAGER_ID	PHONE_NUMBER	SALARY
Reference	159	.3	80	LWOODRUFF	Lindsey	2005-03-10 00:00:00 SA_REP		Woodruff	146	011.44.1345.729268 8000	
Candidate	159	.3	80	LSMITH	Lindsey	2005-03-10 00:00:00 SA_REP		Smith	146	011.44.1345.729268 8000	
Candidate	161	.25	80	SSEWALL	Sarath	2006-11-03 00:00:00 SA_REP		Sewall	146	011.44.1345.529268 7000	
Candidate	162	.25	80	CVISHNEY	Clara	2005-11-11 00:00:00 SA_REP		Vishney	147	011.44.1346.129268 10500	
Reference	169	.2	80	HELOOM	Harrison	2006-03-23 00:00:00 SA_REP		Bloom	148	011.44.1343.829268 10000	
Reference	170	.2	80	TFOY	Taylor	2006-01-24 00:00:00 SA_REP		Fox	148	011.44.1343.729268 9600	
Reference	198		50	DOCONNEL	Donald	2007-06-21 00:00:00 SH_CLERK		O'Connell	124	603.123.5432 2600	
Candidate	198		50	DOCONNEL	Donald	2007-06-21 00:00:00 SH_CLERK		O'Connell	124	650.507.9833 2600	
Reference	202		20	PFAY	Pat	2005-08-17 00:00:00 MK_REP		Fay	201	603.123.6666 6100	
Candidate	202		20	PFAY	Pat	2005-08-17 00:00:00 MK_REP		Fay	201	603.123.6666 6000	

Schema Mapping

By default, a reference object will be compared with a candidate object in the same-named schema as the reference schema. Using schema mapping, you can optionally compare objects in a reference schema with objects in a different candidate schema. Any schema can only be mapped once. Provide reference and candidate schema names for mapping under the Schema Mapping section of the Data Comparison Specification page. Default candidate schema will then be picked from schema mapping you specified.

You may further override the candidate schema of individual item by editing the item, clicking the Override button next to the Candidate Object field, and explicitly specifying the candidate object belonging to any schema. For such items whose candidate objects are overridden in this way, schema mapping will be ignored.

Usage of Buckets

A bucket is a range of rows in a database object that is being compared. Buckets improve performance by splitting the database object into ranges and comparing the ranges independently. Every comparison divides the rows being compared into an appropriate number of buckets. The number of buckets used depends on the size of the database object and is always less than the maximum number of buckets specified for the comparison by the maximum number of buckets specified.

When a bucket is compared, the following results are possible:

- No differences are found —
The comparison proceeds to the next bucket.
- Differences are found —
The comparison can split the bucket into smaller buckets and compare each smaller bucket. When differences are found in a smaller bucket, the bucket is split into still smaller buckets. This process continues until the minimum number of

rows allowed in a bucket is reached, whereupon a comparison reports whether there are differences in the bucket and identifies each row difference.

You can adjust the maximum number of buckets and minimum rows per bucket to achieve the best performance when comparing a particular database object.

The comparison program uses the `ORA_HASH` function on the specified columns in all the rows in a bucket to compute a hash value for the bucket. If the hash values for two corresponding buckets match, the contents of the buckets are assumed to match. The `ORA_HASH` function efficiently compares buckets, because row values are not transferred between databases. Instead, only the hash value is transferred.

Note: If an index column for a comparison is a `VARCHAR2` or `CHAR` column, the number of buckets might exceed the value specified for the maximum number of buckets.

Additional Setup for Real-time Monitoring

Oracle Enterprise Manager Cloud Control's (Cloud Control) Compliance features include the ability to monitor certain elements of your targets in real time to watch for configuration changes or actions that may result in configuration changes.

These features include Operating System level file change monitoring, process starts and stops, Operating System user logins and logouts, Oracle database changes and more.

The real-time monitoring for these features takes place from the Cloud Control agent. Some of these monitoring capabilities require specific setup steps depending on the type of monitoring you will do and what Operating System is being monitored.

This chapter outlines the specific requirements and pre-requisites that exist to use the Compliance Real-time Monitoring features. For details on how to use Real-time monitoring from Cloud Control, see the chapter Compliance Management in this document. This chapter covers the following topics:

- [Overview of Real-Time Monitoring](#)
- [Overview of Resource Consumption Considerations](#)
- [Configuring Monitoring Credentials](#)
- [Preparing To Monitor Linux Hosts](#)
- [Preparing To Monitor Windows Hosts](#)
- [Preparing To Monitor Solaris Hosts](#)
- [Preparing to Monitor AIX Hosts](#)
- [Preparing To Monitor the Oracle Database](#)
- [Setting Up Change Request Management Integration](#)
- [Overview of the Repository Views Related to Real-time Monitoring Features](#)
- [Modifying Data Retention Periods](#)
- [Real-time Monitoring Supported Platforms](#)

29.1 Overview of Real-Time Monitoring

Real-time monitoring is configured through the Cloud Control Server. Users with the EM_COMPLIANCE_DESIGNER role create Compliance Standard Rules that are of type "Real-time Monitoring Rule." These rules are then associated with Compliance Standards and these standards are subsequently associated with one or more targets.

After the Compliance Standard to target association is complete, the set of monitoring rules are sent to the agent to enable real-time monitoring. All monitoring for Real-time monitoring occurs on the agents and all observed action data is sent from the agent to the Cloud Control server for reporting and data management.

29.2 Overview of Resource Consumption Considerations

The Real-time monitoring features are built into the Cloud Control agent. There are some specific resource considerations if you use the Real-time monitoring features. The following sections describe issues you should consider when using Real-time monitoring features.

29.2.1 OS File Monitoring Archiving

An optional setting when monitoring for file changes in real time is to make an archive copy of the file on the agent. When monitoring first begins, a copy of the file at that time is made and stored into a private directory in the ORACLE_HOME directory of the agent. Then, any subsequent changes to that file will result in additional copies of the file being archived in that same directory. This feature allows you to later perform a file diff from the user interface or to issue a job to roll back a file to a previous version.

This feature however will use disk space to make copies of the file. Care should be taken to ensure that this feature is only enabled for files that are critical. During rule creation, the user can specify how many copies of a file to save. The default is five historic versions. This can also be adjusted to tune potential resource consumption.

Select the checkbox in the Ignore Events Prior to Rule field to ignore all previous Oracle database change events when the Oracle database monitoring module runs the first time.

29.2.2 OS File Read Monitoring

The Operating System File level monitoring can monitor many types of changes to files, but can also monitor reads to files. If you have a Rule to monitor a facet that has file patterns that are read frequently, this may result in a very large number of observations. You can reduce the number of observations by ensuring that your Rule includes a filter on either time or a user that you want to ensure does not read the file.

For instance, monitoring the */etc/passwd* file for reads for All users will result in many observations being created. However, if you only monitor the */etc/passwd* file by a specific user, you can create a user filter for this specific user during rule creation. You will then only receive an observation when that specific user attempts to read the file.

29.2.3 Creating Facets That Have Very Broad Coverage

It is possible to create a facet for any entity type (Operating System File for instance) that monitors every entity (for example every file on the OS, or every user login). This will result in increased overhead on the agent as well as significant numbers of observations coming into the Cloud Control Server. It is important to remember that facets are created to specify files that are very important to monitor for security/compliance purposes. For instance, monitoring all modifies to a log file that change every few seconds will add a great deal of resource usage to the agent and server. Instead, in this case, it may be appropriate to create a rule to monitor the log file for all changes, but filter only when the log change is made by a non-application user. This would only capture the log file change if a regular user attempted to change

or tamper with the log rather than when the log is simply being updated by an application.

29.2.4 Cloud Control Repository Sizing

Database sizing considerations for Real-time monitoring depend on several factors. The most important factor is the number of observations expected in a month. The second factor is the number of months data will be retained in the repository. Repository retention rates are explained in the Enterprise Manager Administration Guide.

In general, each observation consumes roughly 1.5KB of space in the database. This is a guideline and this number can vary depending on many factors for each installation.

For example, if a customer expected a total of 10 million Real-time observations per month across all targets and wanted to retain the data for 12 months, then the database size required for this would be roughly 180GB.

10,000,000 Observations x 12 Months x 1500 Bytes = 180,000,000,000 Bytes

This size represents Real-time monitoring data only and does not include database storage needs for other areas of Cloud Control.

The number of observations to expect per month can vary from environment to environment and can also depend on what types of monitoring are configured. You may be required to tune the expected size over time after Rules and Facets have been enabled for some time and configured to fit the organizations requirements. You can easily find your observations usage over a month by selecting **Compliance** from the **Enterprise** menu, then choosing **Browse By Systems UI Report** from the **Real-time Observations** page to select your systems and see the related counts of observations for each system over a period of time.

29.3 Configuring Monitoring Credentials

Many of the real-time monitoring capabilities require monitoring credentials that maintain the ability to launch monitoring programs with root privileges. These processes that Real-time monitoring uses begin with the prefix *nmxc*. Low-level monitoring uses operating system APIs that are not available to regular users.

Before starting to use the Real-time monitoring features on a target host for the first time, the following settings must be configured from the Enterprise Manager Console.

1. Ensure that the agent's *root.sh* script is run after agent installation.

After installing the agent, the *root.sh* script must be run as the root user. This script must be run before configuring the rest of these credential steps.

2. Configure Privilege Delegation.

Privilege Delegation settings are found from the **Setup** menu by choosing **Security**, then **Privilege Delegation**. On this page you can either set privilege delegation for each host manually or you can create a Privilege Delegation Setting Template.

Privilege delegation for each host that will have real-time monitoring must have SUDO setting enabled with the appropriate SUDO command filled in (for example, */usr/local/bin/sudo*).

3. Configure Monitoring Credentials.

Monitoring Credential settings are found from the Setup menu. Choose **Security** then **Monitoring Credentials**. From this page, select the Host target type and click **Manage Monitoring Credentials**.

For each entry with the credential “Host Credentials For Real-time Configuration Change Monitoring”, select the entry and click **Set Credentials**. You will be asked for a credential set to use. Ensure you also add “root” to the Run As entry. If “Run As” is not visible, then the privilege delegation was not set properly in the previous step.

To set monitoring credentials in bulk on multiple hosts at once, you can use EMCLI. For more information on using EMCLI to set monitoring credentials, see the section, *Managing Credentials Using EMCLI* in the Security chapter of *Oracle Enterprise Manager Administration*. Likewise, for more information about configuring monitoring credentials in Cloud Control, the Security chapter of *Oracle Enterprise Manager Administration*.

29.4 Preparing To Monitor Linux Hosts

The following sections describe how to prepare Linux hosts for monitoring.

29.4.1 OS File Monitoring

Before using Real-time file monitoring for Linux, a loadable kernel module must be installed on the host. This loadable kernel module provides you with the most efficient way of monitoring the host. This loadable kernel module is referred to as the File Audit Module, or Audit Module for short.

Acquiring the Kernel Module

The kernel audit module is available from <http://oss.oracle.com/projects/fileauditmodule>. There are two ways to get the file audit kernel module:

1. **Prebuilt .ko files** for which Oracle has already prebuilt, you can use this in your environment. You can look for the Prebuilt kernel modules under the **Downloads** link. To find the matching prebuilt version, run the `uname -r` command on the host being monitored and compare that version to the version of the prebuilt modules. The complete version string must match perfectly. For 32-bit machines, the post-fix of the .ko file name will be .ko. For 64-bit machines, the post-fix of the .ko file name will be .k64.ko.
2. **Build your own kernel module.** To build your own kernel module, you can download the following RPM from the **Downloads** link:

Fileauditmodule-emversion-revision-noarch.rpm

You should always retrieve the latest revision available at the time you are installing this module. The emversion field must match the version of Cloud Control agent and server you are using.

Install this RPM on the host you want to monitor as root. The installation of this RPM depends on the kernel-devel package matching your running kernel also existing on the host. This kernel-devel package comes with the same media as the Linux installers.

In addition to installing this package, you must ensure that the version of gcc available on your host matches the version with which the kernel was built. To do this, view the `/proc/version` file to see what gcc version the kernel was built with

and then run the command `gcc -v` to see what version of `gcc` is being used. These two versions should match.

Also check that the file `/boot/System.map-{version}` exists where `{version}` must match the kernel version you see when you run the `uname -r` command. This file contains system symbols that are required to decode the kernel symbols we are monitoring for real-time changes. Without this file, real-time file monitoring will not function. This file is standard on all default Linux installations.

After installing this package and checking prerequisites successfully, go to the directory where the package contents were installed (defaults to `/opt/fileauditmodule`) and run the following script:

```
compmod.sh
```

This will build the kernel module file (`.ko`, `.k64`, or `.o` extension depending on the OS version) and place it in the `/opt/fileauditmodule` directory.

If the audit module file is not created, check the `make.log` and `build.log` files for any errors in building the module.

If all of your hosts have the exact same kernel version as shown using the command `uname -r`, then you only need to compile the module on one machine. You can then copy the `.ko`, `.k64`, or `.o` file to the other servers without having to build on that specific host.

Deploying the Kernel Module

Once you have either the prebuilt `.ko` file or a `.ko` file that exists from building it from the source RPM, the `.ko` file must be located in the proper directory. The default location for this file is in the `bin` folder under the agent home directory. You can also place the file in any location on the host and change the `nmxc.properties` file under the `AGENT_INST/sysman/config` directory of the agent home. The property `nmxcf.kernel_module_dir` specifies the absolute path to the `.ko` directory.

Install Kernel Module Job

In addition to manually placing the `.KO` file on the agent, there is a Cloud Control job named *Real-time Monitoring Kernel Module Installation*. This job is configured with a list of Linux hosts on which you can install the kernel module. It will search in a directory locally on the Cloud Control server disk for prebuilt `.ko` files or the source RPM file. If it finds a matching prebuilt `.ko` file, it will send this to the matching agents; otherwise it will send the RPM to the agent and install and compile it resulting in a new `.KO` file.

Prior to using this job, files from `OSS.ORACLE.COM` must be manually retrieved by the user and placed into the `%ORACLE_HOME%/gccompliance/fileauditmodule/resources/linux` directory. This directory already exists on the server with a `README` file indicating this is the location to place these files. The files that must be placed here are either prebuilt `.KO` files or the source RPM file. If you have built your own `.KO` files in your environment, you can also place those `.KO` files into this directory on the server and deploy it to other hosts in your environment.

Special Considerations for Enterprise Linux 5 and Greater

For Enterprise Linux 5 and greater, the kernel audit module is not required. The monitoring will use the built-in audit subsystem if a kernel module is not detected at startup time. However, the functionality of the audit subsystem is not as robust as the capability that the kernel audit module can provide.

You will lose the functionality that provides the granularity of what type of change there has been to a file, whether it was a create action or a modify action. Without the kernel module, all changes to a file will appear as a modify action. Additionally, monitoring a directory that does not exist yet or a directory that may exist now and gets removed later may be disrupted since the underlying Linux audit subsystem does not handle these cases.

It is recommended that you use the kernel audit module even with the newer versions of Linux, if possible.

29.4.2 Debugging Kernel Module Or Other File Monitoring Issues

You may detect a problem with the kernel module in a few different ways:

1. You may have noticed that you do not receive real-time file changes on the Enterprise Manager console for file changes that you know should occur.
2. In the Compliance Standard Target Associations or Real-time Observations page on the user interface, you may see an agent warning indicating a kernel module problem.
3. When examining the *nmxcf.log* file under *AGENT_INST/sysman/logs*, you may see errors indicating that the kernel module could not be loaded or used for various reasons.

If you encounter any of these issues, most likely there was a problem with compiling or inserting the Linux kernel module at run time.

You can confirm whether the auditmodule was loaded properly by running the following command.

```
grep -i auditmodule /proc/modules
```

If you do not receive any output, then the auditmodule is not loaded and the agent will not perform real time file monitoring.

If the audit module file was generated properly and it does not show up in the module list above, you can attempt to manually load the module to see if there are any errors. Use the following command where you replace {audit module file name} with the entire name of the .ko file that was created from *compmod.sh*:

```
insmod {audit module file name}
```

If you experience no errors during this command, you can check the module list again by using the `grep` command above. If the audit module now appears, then the file monitoring capability should work. An agent restart is necessary; however there still may be a problem with the file monitoring process finding the .ko file which you will experience again next time your host is rebooted.

One additional step to debug any issues with the file monitoring process is to try to run it manually. To do this, follow these steps:

1. Get the process ID of the agent TMMain process:

```
ps -eaf |grep TMMain
```
2. Execute the nmxcf process using the following command replacing the values in {} with the proper path elements or the process ID from the previous command:

```
sudo {agent_home}/core/{agent_version}/bin/nmxcf -e {agent_
home}/agent_inst/ -m {agent_home}/agent_
inst/sysman/emd/state/fetchlet_state/CCCDATAFetchlet -w {process id of
TMMAIN}
```

Running the nmxcf process this way will not work in the long term since it will not start up again when the agent is restarted, but this can help in trying to debug any issues as to why the process cannot start.

If the module still is not able to load and if you need to contact Oracle support about the issue, please be sure to include the following information with your support ticket:

- Output of the command: `uname -a`
- Output of the command: `grep -i auditmodule /proc/modules`
- Output of the command: `rpm -q -a |grep -i kernel-devel`
- The `make.log` and `build.log` files from the `/opt/fileauditmodule` directory where you ran `compmod.sh` if you built your own `.ko` file
- The files `AGENT_INST/sysman/log/nmxc*.log`
- Any warnings or errors you received when trying to start nmxcf manually.

This information will help Oracle Support to determine if the real time file monitoring audit module of the agent can be built on your environment.

Warning: Be careful when using the Linux OS command `rmmod` which is used to unload a kernel module. If the nmxcf binary is running and you use `rmmod`, there is a chance that a kernel panic can arise by trying to unload a kernel module in use. The use of `rmmod` in Linux should be done carefully no matter which module you are unloading.

29.5 Preparing To Monitor Windows Hosts

The Real-time monitoring features support Windows 2003 and 2008 Server along with Windows XP. The Real-time monitoring modules for Windows rely on various capabilities of the operating system to collect all of the information on actions. One part of this is to capture the user that made changes from the Windows Event Log. If you do not configure Windows to capture users that make changes, the agent will not capture this information. However it will still capture that a change occurred and when it occurred.

To configure the event log to work with real time monitoring, perform the following steps:

1. From Windows Explorer, select the directory that is being monitored by a Real-time Monitoring Rule, right-click and select **Properties**.
2. Go to the Security tab.
3. Click **Advanced**.
4. Select the Auditing tab.
5. Click **Add**. (In Microsoft XP, double-click the **Auditing Entries** window).
6. Select the Name **Everyone**, then click **OK**. You can also choose specific users if you are only monitoring for changes by specific users in Configuration Change Console rules. The rules filter the results by user as well, so even if you enable audit for everyone, only users that you want to monitor changes of in your rules will be captured.
7. Select the following options (Successful and/or Failed) from the Access window:
 - Create Files/Write Data

- Create Folders/Append Data
 - Delete Files Subfolders and Files
 - Delete
8. Click **OK** to exit.
 9. Repeat steps 1 through 7 for all other monitored directories and/or files.
 10. From the **Start** menu, select **Settings**, then **Control Panel**, then **Administrative Tools**, then **Local Security Policy**, then **Local Policies**, then **Audit Policy**. Double-click and turn on the following policies (Success and/or Failure):
 - Audit account logon events
 - Audit logon events
 - Audit object access
 11. Close the Local Security Settings screen.
 12. From the **Start** menu, select **Settings**, then **Control Panel**, then **Administrative Tools**, and finally **Event Viewer**.
 13. Select **System Log**, then click **Action** from the menu bar and select **Properties**.
 14. From the System Log Properties panel, on the General tab, set the Maximum log size to at least 5120 KB (5 megabytes) and select **Overwrite Events as Needed**. Note that the log size depends on the number of events generated in the system during a two-minute reporting interval. The log size must be large enough to accommodate those events. If you extend the monitoring time for file events because you expect the change rate to be lower, you need to ensure that the audit log in Windows is large enough to capture the events.
 15. Click **Apply** then **OK** to exit.

If Windows auditing is not configured properly, you will see warnings on the Compliance Standard Target Association page on the Cloud Control user interface. This is the same page where you associated your Real-time Monitoring compliance Standards to your targets.

29.5.1 Verifying Auditing Is Configured Properly

To verify that the host records login and logout events, follow these steps:

1. Log out of the host and then log back into the host.
2. From **Start**, select **Settings**, then **Control Panel**, then **Administrative Tools**, and finally **Event Viewer**.
3. Select **Security Log** and choose **Filter** from the **View** menu. Select **Security for the Event Source** and **Logon/Logoff** for the Category fields.
4. Click **OK**.

The Event Viewer should have the activity recorded as Event 528.

29.5.2 Subinacl External Requirements

As mentioned earlier, the agent will send warnings to the server when audit settings are not set properly. It, however, can only do this if the windows feature SUBINACL is installed. If this feature is not installed on the host, a warning will be sent to the server saying that the agent cannot detect whether audit settings are correct. This warning will be visible from the Compliance Standard Associate Targets page.

You can specify the absolute path to the directory that contain subinacl by setting the following property in the `AGENT_INST/sysman/config/nmxc.properties` file:

```
nmxcf.subinacl_dir=
```

SubInACL is available for download from Microsoft's Web site.

29.6 Preparing To Monitor Solaris Hosts

Real-time monitoring on Solaris systems utilizes the Solaris audit system which is part of the Solaris Basic Security Model (BSM). BSM auditing allows system administrators to monitor events and to detect user account logins and logouts as well as file changes.

Verify that BSM auditing is enabled by running the following command with root privilege:

```
/usr/sbin/auditconfig -getcond
```

You should see the following output:

```
audit condition = auditing
```

If the output is different from the above, it means the BSM auditing needs to be enabled through different methods in different Solaris releases.

29.6.1 Enabling BSM Auditing

You can enable BSM auditing using the steps below for each of the following environments.

29.6.1.1 Using Solaris Versions 9 and 10

To enable BSM auditing, you can use the following command with root privilege:

```
/etc/security/bsmconv
```

See the Solaris BSM Auditing manuals for additional details on setting up BSM auditing.

If auditing is already enabled on the server, simply verify that the audit system configuration matches the configurations detailed below.

The audit file can be configured to include specific events. The `/etc/security/audit_control` file controls which events will be included in the audit file. This section summarizes the configuration; for further details, refer to the Sun Product Online Documentation site.

For monitoring entity types OS FILE (file changes) and OS USER (user logins/logouts), the flags line in the file `/etc/security/audit_control` should be set as follows:

```
flags: +fw,+fc,+fd,+fm,+fr,+lo
```

This configuration enables success/fail auditing for file writes (fw), file creates (fc), file deletes (fd), file attribute modifies (fm), file reads (fr) and login/logout events (lo); where '+' means to only log successful events.

If you are interested in logging the failed events as well, remove the '+' sign before each event in the flag.

Note: Installing BSM on an existing host has the requirement that the host is rebooted.

Auditing Users: The `audit_user` file controls which users are being audited. The settings in this file are for specific users and override the settings in the `audit_control` file, which applies to all users.

Audit Logs and Disk Space: The `audit_control` file uses entries to control where the audit logs are stored and the maximum amount of disk space used by the audit system. The minimum requirement for file monitoring is approximately 10 minutes worth of data stored on the hard drive or the configured reporting interval time.

29.6.1.2 Using Solaris 11

Auditing is enabled by default on Solaris 11, but only user login/logout events are monitored by default. For monitoring both the OS File change events and OS USER logins/logout events, you can execute the following command with root privilege:

```
/usr/sbin/auditconfig -setflags fw,fd,fc,fm,fr,lo
```

The configuration flags have the same meaning as defined in the last section.

Note: This configuration will not affect the existing sessions in which users already log into the host, so you must terminate all the existing sessions and then re-login or simply reboot the machine to ensure this change takes effect.

As the `bsmconv` command has been removed on Solaris 11, you can use the following command to enable the auditing feature, if needed:

```
audit -s
```

29.6.2 Managing Audit Log Files

Cloud Control Real-time Monitoring only reads the audit logs; it does not delete the logs. This might flood the system with log files and prevent it from logging additional events. To manage and delete old audit events while maintaining minimum monitoring requirements, follow these steps:

1. The auditing policy can be set to automatically drop new events (keeping only a count of the dropped events) rather than suspending all processes by running the following command:

```
# auditconfig -setpolicy cnt
```

2. Run the following command to force the audit daemon to close the current audit log file and use a new log file:

```
/usr/sbin/audit -n
```

3. Run the following command to merge all existing closed auditing log files into a single file with an extension of `.trash` and then delete the files:

```
/usr/sbin/auditreduce -D trash
```

4. Create a cron job to periodically run the commands in Step 2 and 3 above. The frequency at which these two commands are run can be adjusted based on the anticipated event volume and the amount of disk space allocated to auditing. The only requirement is that the time between the `audit -s` command and the

`auditreduce` - D trash command is at least 15 minutes or twice the reporting interval if that is changed.

29.7 Preparing to Monitor AIX Hosts

Real-time monitoring on AIX systems utilizes the underlying AIX audit subsystem provided by the OS. IBM AIX 5.3 and 6.1 are the only currently supported versions.

29.7.1 Installation Prerequisite for AIX 5.3

Before using Real-time monitoring on AIX 5.3 hosts, ensure that you are using AIX 5.3 5300-08 service pack or higher. This maintenance package is available from IBM.

29.7.2 Administering AIX Auditing

The AIX auditing subsystem allows an administrator to record security-relevant information, such as User Logins, Logouts, and file changes, for analysis against existing security policies and detection of security violations.

Setting up auditing involves modification of the existing auditing configuration files. To set up auditing, follow these steps:

1. Log into the AIX machine as the root user.
2. Open a terminal window and change directory to `/etc/security/audit`
3. Open the config file in `vi`.
4. Locate the following sections, and update or add the listed values:

```
start:
binmode = off
streammode = on
...
classes:
...
filewatch = PROC_Create,PROC_Delete,FILE_Open,FILE_Write,FILE_Close,FILE_
Link,FILE_Unlink,FILE_Rename,FILE_Owner,FILE_Mode,FILE_Fchmod,FILE_Fchown,FS_
Chdir,FS_Fchdir,FS_Chroot,FS_Mkdir,FS_Rmdir,FILE_Symlink,FILE_Dupfd,FILE_
Mknod,FILE_Utimes
users:
root = filewatch
default = filewatch
```

Note: In this case default refers to all users that are not root. Further note that the last line of the config file should be a blank line.

5. Save your modifications and exit `vi`.
6. In the same directory (`/etc/security/audit/`) open the file `streamcmds` in `vi`.
7. Clear all text from the file. The default configuration for this file is not necessary, as the File Monitoring agent module (`nmxcf` process) will operate as a direct audit reader. Clearing the file helps to reduce CPU usage and improve overall auditing performance.
8. Save the file and exit `vi`.
9. At the terminal prompt, enter the following command to initialize Auditing at system startup:

```
mkitab "audit:2:once:/usr/sbin/audit start"
```

10. At the prompt, restart audit using the command `/usr/sbin/audit shutdown` and `/usr/sbin/audit start` or directly reboot the host to make the auditing effective.

29.7.3 Verifying AIX System Log Files for the OS User Monitoring Module

The OS User monitoring module relies on the following system log files:

- `/etc/security/failedlogin`
- `/var/adm/wtmp`
- `/var/adm/sulog`

Be sure the log files exist before running the OS User monitoring module on an AIX host. If any of the log files is missing, refer to the AIX System documentation for more information about how to generate it.

29.8 Preparing To Monitor the Oracle Database

This section describes the steps involved in setting up auditing within an Oracle database. If you are going to monitor an Oracle database with any of the Oracle entity types, you will need to perform these steps before events will be captured.

Before configuring auditing it is suggested you review the Auditing Database Use section of the *Oracle Database Administrator's Guide*. This document provides an overview of Oracle's auditing functionality, as well as basic concepts and guidelines for auditing configurations. Note that this document does not cover all details of configuring and fine tuning the Oracle audit system. Instead, this document serves as an example of the basic steps involved to configure the Oracle audit system to enable Real-time monitoring through Real-time monitoring rules.

29.8.1 Setting Auditing User Privileges

When you create a Real-time Monitoring Compliance Standard Rule to monitor an Oracle instance target, the agent will read the audit trail to perform its monitoring.

Real-time monitoring for Oracle entity types requires the audit trail to be stored in the database as opposed to a file. To verify if a setting is correct, follow these steps:

1. In Cloud Control, go to the target home page for the Oracle Database target for which you want to enable Real-time Monitoring.
2. From the **Administration** menu, select **Initialization Parameters**.
3. Log in to the database as a sys user, connecting as SYSDBA.
4. Find the parameter `audit_trail` and ensure it is set to DB. If not, this parameter needs to be changed in the Oracle Database.
5. This change will require a restart of the database.

29.8.2 Specifying Audit Options

Through SQL plus, an Oracle DBA can use `audit` and `noaudit` statements to configure audit options for the database. The `audit` statement allows you to set audit options at three levels:

Table 29–1 Audit Options Table

Level	Effect
Statement	Audits specific SQL statements or groups of statements that affect a particular type of database object. For example, AUDIT TABLE audits the CREATE TABLE, TRUNCATE TABLE, COMMENT ON TABLE, and DELETE [FROM] TABLE statements.
Privilege	Audits SQL statements that are executed under the umbrella of a specified system privilege. For Example, AUDIT CREATE ANY TRIGGER audits statements issued using the CREATE ANY TRIGGER system privilege.
Object	Audits specific statements on specific objects, such as ALTER TABLE on the employee table

To use the audit statement to set statement and privilege auditing options a DBA must be assigned AUDIT SYSTEM privileges. To use the audit statement to set object audit options, the DBA must own the object to be audited or be assigned the AUDIT ANY privilege within Oracle. Privilege assignments are covered in the following section.

Audit statements that set statement and privilege audit options can also include a BY clause to supply a list of specific users or application proxies to audit, and thus limit the scope of the statement and privilege audit options.

Some examples of audit statements can be seen below. Feel free to use these as a basis for the audit settings you specify within your database. Once all audit settings are in place you can create application policies, using the Oracle (SQL Trace) agent module with which to monitor the Oracle database instance.

Statement Audit Options (User sessions)

The following statement audits user sessions of users Bill and Lori.

```
AUDIT SESSION BY scott, lori;
```

Privilege Audit Options

The following statement audits all successful and unsuccessful uses of the DELETE ANY TABLE system privilege:

```
AUDIT DELETE ANY TABLE BY ACCESS WHENEVER NOT SUCCESSFUL;
```

Object Audit Options

The following statement audits all successful SELECT, INSERT, and DELETE statements on the dept table owned by user jward:

```
AUDIT SELECT, INSERT, DELETE ON jward.dept BY ACCESS WHENEVER SUCCESSFUL;
```

Example Oracle Audit Monitor Configurations

The following command audits all basic statements. Extra statements are not audited.

```
Audit all by access;
```

The following statement audits all extra statements:

```
audit ALTER SEQUENCE, ALTER TABLE, DELETE TABLE, EXECUTE PROCEDURE, GRANT
DIRECTORY, GRANT PROCEDURE, GRANT SEQUENCE, GRANT TABLE, GRANT TYPE,
INSERT TABLE, LOCK TABLE, UPDATE TABLE by access;
```

The following command displays audit settings for statements:

```
SELECT * FROM DBA_STMT_AUDIT_OPTS;
```

Once you have specified your audit configuration you can then create real-time monitoring rules from the Cloud Control Server that uses the Oracle Database entity types.

29.9 Setting Up Change Request Management Integration

This section explains how to install and configure integration with a Change Management Server and to be able to determine whether changes that occur are authorized automatically.

29.9.1 BMC Remedy Action Request System 7.1 Integration

Remedy ARS 7.1 is a supported Change Management system for automatic reconciliation of observations. The following steps outline how to setup Remedy and also configure the integration with Cloud Control.

29.9.1.1 Remedy Installation and Customization

Follow these steps to install and customize Remedy ARS 7.1.

1. Install Remedy ARS 7.1. Ensure the following components are all installed and properly licensed:

ARS 7.1.00 Patch 011

Midtier 7.1.00 Patch 011

Flashboard Server 7.0.03

Assignment Engine 7.1

Asset Management 7.0.03*

CMDB 2.1.00 Patch 4

CMDB Extension Loader

Approval Server 7.1

Change Management Server 7.0.03 Patch 008*

Problem Management Server 7.0.03*

Incident Management Server 7.0.0*3

User Client

Administrator Client

These packages all come with the IT Service Management Pack. Oracle provides example customizations for the Remedy under ITSM 7.0.03 Patch 008 environment. For different versions, the customizations may need to be adjusted to account for changes in the version of Remedy.

2. Install the Cloud Control EMCLI_Client on the same host on which Remedy is installed. This will need to be able to communicate to your Cloud Control Server.
 - a. Log in to the Enterprise Manager console.
 - b. Choose **Setup**, then select **Command Line Interface** from the **My Preferences** menu.
 - c. Click **Download the EM CLI kit to your workstation** and download the jar to your Remedy server.

- d. Follow the steps given on the page to install the EMCLI client on the Remedy server.
3. Get the latest version of the Change Request Management connector self-update package. Also acquire the latest version of the example Remedy ARS customizations for Cloud Control version 12c.

These definition files provide a guideline of customizations that must be made in your environment for the integration. These customization files assume a fresh install of Remedy ARS. When integrating with a production instance of Remedy, care should be taken to make sure these customizations are compatible with any previous customizations that have been made to the Remedy instance.

- ActiveLinks_Customization.def
 - Forms_Customization.def
 - Menus_Customization.def
 - Webservices_Customization.def
4. Install the four definition files (.DEF) files in the running Remedy environment by completing these steps:
 - a. Log into the Remedy Administrator tool.
 - b. Select the **Remedy** instance from the hierarchy on the left.
 - c. From the **Tools** menu, select **Import Definitions**, then select **From Definition File...**
 - d. Select the definition file to import from the list above.
 - e. Check the box labeled **Replace Objects on the Destination Server**.
 - f. Choose the drop down option **Replace With New Type**.
 - g. Click **Import**.
 - h. You should not encounter any errors during this process. At the end of import there should be an Import Complete message.
 - i. When done, repeat for the rest of the customization files.
 5. Customize Web Services.
 - a. Log into Remedy Administrator tool.
 - b. Select **Webservices**, then select the webservice **EMCCC_GetCR**. Right click, then select **Open**.
 - c. Select the **WSDL** tab.
 - d. In the input on top, modify the midtier_server and servername values in the **WSDL Handler URL**.
 - e. If midtier is on localhost, you can enter localhost right after http://.
 - f. If the midtier uses port 80, you can omit the port, otherwise include the port after the server name.
 - g. For the servername after "public/", enter the name of the Remedy server.
 - h. Click **View**.
 - i. You should see an XML representing the webservice WSDL file for the webservice.

- j. If you see an error, check the midtier_server name, port, or servername. Also, you can try adding/removing the domain part of the servername.
 - k. If you see the XML content after clicking View, then close this window and save the changes.
 - l. Repeat all above steps with the webservices EMCCC_PublishCSData and EMCCC_UpdateChangeRequest.
 6. Customize Active Links.
 - a. Log in to Remedy Administrator tool.
 - b. Select active links and then select the active link **EMCCCC_ApprovedCR**. Right click, then select **Open**.
 - c. Click the **If Action** tab.
 - d. Click the Current Action **Run Process** at the end of the list of actions.
 - e. In the Command Line field, change the path to *emcli.bat* to match that of where you installed the emcli on the local host.
 7. Create a user in Remedy that will be used for creating requests that will be used for automatic observation reconciliation:
 - a. Log in to BMC Remedy User Client as an administrative user.
 - b. Click **Application Administration Console** on the User Client Home Page.
 - c. Click **Create** for each step 1 through 4 in this wizard.
 - d. When adding the person, add the support group under the Support Groups tab.
 - e. Under the Support Groups Tab, select sub tab **Support Group Functional Roles**.
 - f. Add Support groups with functional role of *Infrastructure Change Management*. Without this, you will not be able to create change requests as the Infrastructure Change Manager fields support group will not have values.
 - g. Go to AR System Administrator Console.
 - h. On the left side bar, select **Application**, then **Users/Groups/Roles**, then **Select Users**.
 - i. This will load the user search page. Click **Search** at the top right.
 - j. Double-click the newly created user above to bring up the user form.
 - k. Click the down arrow next to "Group List" field and select **Infrastructure Change Master**.
 - l. Repeat the previous step and add the following Groups to this user as well.
 - Infrastructure Change Submit
 - Infrastructure Change User
 - Infrastructure Change Viewer
 - m. Save the changes to this user by clicking the **Save** button in the upper right hand corner of the window.

29.9.1.1.1 Adding the Connector to Cloud Control

Follow these steps to add the connector to Cloud Control.

1. Add the Change Management Connector to Cloud Control.
 - a. Log into Enterprise Manager as an Administrative user that has privileges to create a connector.
 - b. From the **Grid** menu, select **Provisioning and Patching**, then choose **Software Library**.
 - c. Click **Actions**, then select **Administration**.
 - d. Click **Add**.
 - e. Provide a name, such as "self update swlib".
 - f. Provide a location where the swlib files will be located on the Cloud Control server. This can be anywhere, but must be a path that the Cloud Control user can access. You must put the full absolute path in this input.
 - g. This process will take several minutes to complete.
 - h. Locate the connector self-update package file.
 The connectors jar can be downloaded from the Cloud Control store to EM@Customer using the Self Update console, and can be exported to any local directory using the export functionality of Self Update.
 - i. Run: `emcli import_update -file=<full path>/connector.zip -omslocal` (where *connector.zip* is an example name of the self update package)
 - j. If you have errors with the previous step, make sure the user you run `emcli` as has permissions to access this directory and file. Also, be sure you are using absolute path for the *-file* switch.
 - k. When successful, you will receive the following message:
Operation completed successfully. Update has been uploaded to Cloud Control. Please use the Self Update Home to manage this update.
 - l. Log into the Enterprise Manager console.
 - m. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
 - n. Find the type "Management Connector" and click the link "1" under "Downloaded Updates" for this entry.
 - o. Select the Connector from the table and click **Apply**.
2. Create a Change Management Connector instance.
 - a. Log in into Enterprise Manager console.
 - b. From the **Setup** menu, select **Extensibility**, then select **Management Connectors**.
 - c. Select "Remedy Change Management Connector" from the drop-down after "Create Connector", then click **Go**.
 - d. Provide a name and description for the connector. This name is used to choose the connector when creating a Real-time Monitoring Compliance Standard Rule.
 - e. After returning to the management connector listing page, select the newly added row, then click **Configure**.
 - f. Under the Web Service End Points label, change the [servername] and [port] to match that of your Remedy instance Web Services. The values you put here

will be similar to what you configured in the Web Services step earlier in these instructions.

- g.** Enter the Remedy username and password you are using for the connector integration.
- h.** Enter the locale ('en', for example).
- i.** Enter the time zone offset of the remedy server from UTC, ('-08:00', for example).
- j.** Enter the Change ID to use as a test. This should be a valid Change Request ID currently existing in Remedy that is used to test the connectivity between Cloud Control and Remedy.

29.9.1.1.2 Using Automatic Reconciliation Rules

Once Remedy is customized and the Cloud Control connector is configured, to utilize the automatic reconciliation features you need to create Real-time Monitoring Rules that are configured to use automatic reconciliation. Use the following steps:

- 1.** Create a Real-time monitoring Rule:
 - a.** Follow the normal steps to create a Real-time monitoring Rule.
 - b.** On the Settings page, choose **Authorized Observations Automatically** using Change Request Management System. This configures Cloud Control to use this change request from Remedy for reconciliation of Real-time Observations that are detected.
 - c.** Select the connector from the drop-down.
 - d.** Click to annotate change requests with authorized observations check box.
 - e.** Continue to save the rule after this. The Real-time Monitoring Rule can be used like any other Real-time Monitoring rule. Create a Compliance Standard, add this rule to the Compliance Standard, and associate this compliance standard to one or more targets.

The configuration of rules is discussed in more detail in the Compliance Management section.

29.9.1.1.3 Creating Change Requests for Upcoming Changes

Now that integration is set up and Real-time monitoring rules have been created, Change Requests can be created by Remedy users in the Remedy interface. These Change Requests will be compared to observations that occur to automatically determine if these observations are from actions that were authorized by change requests or not.

To make this correlation, some new fields that have been added to the Change Request form must be filled out by the change request filer. Not all fields are required; correlation only occurs on the fields that are present in the Change Request.

For instance, the following fields have been added to the Change Request form under the Oracle Enterprise Manager Integration tab:

- **Connector:** Choose the Cloud Control connector this Change Request will use to integrate with Cloud Control.
- **Hostname:** the hostname(s) this change request is for. These are the hosts that this change request is specifying someone needs to make changes to. An empty value in this field indicates that all hosts will be correlated to this change request.

- **Target User List:** the user name(s) this change request is for based on target users. These are the target users you expect to log in to the target to make a change. An empty value in this field means that all users on the target will be correlated to this change request.
- **Target Type:** the target type this change request is against. An empty value in this field means that any target type will be correlated to this change request.
- **Target:** The target this change request is specifically for. An empty value in this field indicates that any target will be correlated to this change request.
- **Facet:** The facet this change request is specifically for. An empty value in this field indicates that all facets on the above target type and target will be correlated for this change request.

When creating a change request that you want to use to authorize changes detected by Real-time monitoring rules, follow these steps in addition to whatever requirements your organization implements for creation of Change Requests:

1. Under the Dates tab of the Change Request form, fill out the Scheduled Start date and Scheduled End Date. These are the date ranges the request is valid for reconciliation. If an action occurs outside this time, it is marked as unauthorized by the Real-time Monitoring feature.
2. Select the Oracle Enterprise Manager **Integration** tab.
3. Select the Cloud Control connector from the drop-down list.
4. Optionally select values for the five reconciliation criteria as described above: Hostname, Target User List, Target type, Target and Facet. The last three -- Target Type, Target, and Facet -- will be Choice lists based on content in Real-time Monitoring Rules that have been created in Cloud Control that belong to Compliance Standards which are associated to targets. You can add multiple values separated by commas.

Note: This form can be customized in Remedy to look differently. The example form elements from the customizations loaded earlier are only examples.

5. Change the auditable status to True. This configures Remedy to allow Cloud Control to use this change request for reconciliation of Real-time Observations that are detected.
6. Save the change request.
7. A popup displays, notifying you that active links will send the content to Cloud Control. You will see a DOS command window open and then close.

29.9.1.1.4 Overview of Reconciliation Functionality

After creating a change request that references a target and/or facet that is being monitored by Real-time Monitoring rules, any observations that happen against that rule will be correlated to all open and matching change requests.

When the observation arrives at the Cloud Control server, all open change requests that were active (based on Scheduled Start/Stop time) and have matching correlation criteria from the Cloud Control Integration tab will be evaluated. If any change request exists that matches the criteria of the observation, this observation will be marked with an “authorized” audit status. If the annotation check box was checked in

the Rule configuration, details of these authorized observations will be put into a table in the Enterprise Manager Integration tab of the Remedy Change Request.

If no open change requests can be correlated to the observation and the rule was configured to use automatic reconciliation, then this observation is set to an Unauthorized audit status. The Observation bundle to which this observation belonged will be in violation and results in a Cloud Control event being created. This event can further be used through creation of a Cloud Control Event Rule.

An observations audit status can be seen whenever looking at observation details either by selecting Compliance, then Real-time Observations, then Observation Search, or either of the Browse By screens. A user with the proper role can also override the audit status for individual observations from these pages.

Any bundles that are in violation because they contain unauthorized observations will be reflected as violations in the Compliance Results page. These violations cause the compliance score skew lower. If these violations are cleared, the score becomes higher; however, the history of these audit status changes will be retained for the given observation.

29.10 Overview of the Repository Views Related to Real-time Monitoring Features

The following views exist to allow access to Real-time Monitoring data.

View: mgmt\$ccc_all_observations

Description: This view returns all observations that have occurred. Any query against this view should ensure that filtering is done on appropriate fields with *action_time* being the first to take advantage of partitions.

Fields:

Field	Description
OBSERVATION_ID	Unique ID given to the observation when detected by the agent
BUNDLE_ID	Bundle to which this observation belongs based on rule bundle settings
TARGET	Target this observation was found against
TARGET_TYPE	Type of the target
ENTITY_TYPE	Entity type of the entity that had an action against it
ACTION	Action that was observed
ACTION_TIME	Time the action occurred
USER_TYPE	Type of user that performed the action (for example, OS user versus DB user)
USER_PERFORMING_ACTION	Name of the user that performed the action
ORIGINAL_USER_NAME	Previous user name in the case of a SU/SUDO action (only applicable to some entity types)
AFFECTED_ENTITY_NAME	Name of the entity that was affected by this action (file name, and so on)

Field	Description
AFFECTED_ENTITY_PREVIOUS_NAME	Name of the entity prior to the action. For instance for file rename actions, this would be the old file name.
SOURCE_HOST_IP	Source IP of a connection when an action comes from another host (only applicable to some entity types)
ACTION_PROCESS_ID	PID of the process that performed the action (only applicable to some entity types)
ACTION_PROCESS_NAME	Name of the process that performed the action (only applicable to some entity types)
ACTION_PARENT_PROCESS_ID	PID of the parent process of the process that performed the action (only applicable to some entity types)
ACTION_PARENT_PROCESS_NAME	Name of the parent process of the process that performed the action (only applicable to some entity types)
ENTITY_PREVIOUS_VALUE	Previous value of the entity (only applicable to some entity types)
ENTITY_NEW_VALUE	New value of the entity (only applicable to some entity types)
FILE_ENTITY_PREVIOUS_MD5_HASH	Previous MD5 hash value of the entity (only applicable to some entity types)
FILE_ENTITY_NEW_MD5_HASH	New MD5 hash value of the entity (only applicable to some entity types)
AUDIT_STATUS	Current audit status of the observation (unaudited, authorized, unauthorized, and so on)
AUDIT_STATUS_SET_DATE	Date the most recent audit status was set
AUDIT_STATUS_SET_BY_USER	User who set the most recent audit status

View: mgmt\$ccc_all_obs_bundles

Description: This view returns a summary of all observations bundles. Any query against this view should ensure that filtering is done on appropriate fields with *bundle_start_time* being the first to take advantage of partitions.

Fields:

Field	Description
BUNDLE_ID	Bundle to which this observation belongs based on rule bundle settings
TARGET	Target this observation was found against
TARGET_TYPE	Type of the target
RULE_NAME	Name of the Real-time Monitoring Compliance Standard Rule
ENTITY_TYPE	Entity type of the entity that had an action against it
USER_PERFORMING_ACTION	Name of the user that performed the action

Field	Description
BUNDLE_IN_VIOLATION	Boolean value if the bundle currently is in violation. This means at least one observation in the bundle is unauthorized. True indicates the bundle is in violation.
BUNDLE_START_TIME	Date of the first observation in this bundle
BUNDLE_CLOSE_TIME	Date when this bundle was closed
BUNDLE_CLOSE_REASON	Explanation of why this bundle was closed
DISTINCT_OBS_COUNT	Total number of observations in this bundle
AUTHORIZED_OBS_COUNT	Number of observations in this bundle that are currently authorized
UNAUTHORIZED_OBS_COUNT	Number of observations in this bundle that are currently unauthorized
UNAUTH_CLEARED_OBS_COUNT	Number of observations in this bundle that are currently cleared (that were at one point unauthorized)
UNAUDITED_OBS_COUNT	Number of observations in this bundle that are currently unaudited. They have not been evaluated manually or with Change Management integration to determine audit status.

View: mgmt\$ccc_all_violations

Description: This view returns all real-time monitoring violations caused by an observation bundle having at least one unauthorized observation in it.

Fields:

Field	Description
ROOT_CS_ID	Root Compliance Standard GUID. This is used for internal representation of the violation context.
RQS_ID	Runtime compliance standard GUID. This is used for internal representation of the violation context.
RULE_ID	Rule GUID. Internal ID of the rule having a violation.
TARGET_ID	Target GUID. Internal ID of the target having a violation.
ROOT_TARGET_ID	Root Target GUID. Internal ID of target hierarchy.
RULE_TYPE	Type of rule (Repository, Weblogic Server Signature, Real-time Monitoring)
SEVERITY	Severity Level of the rule (Info, Warning, Critical)
BUNDLE_ID	Internal ID of the Observation Bundle that is in violation. This observation bundle has one or more unauthorized observations in it
BUNDLE_START_TIME	Time the Observation Bundle started

Field	Description
BUNDLE_CLOSE_TIME	Time the Observation Bundle closed
TARGET_TYPE	Target Type of the Observation Bundle and all observations inside that bundle.
ENTITY_TYPE	Entity Type of the Observation Bundle and all observations inside that bundle.
USER_NAME	User name that performed the actions in this bundle
AUTHORIZED_OBS_COUNT	Number of Authorized observations in the observation bundle involved in this violation.
UNAUTHORIZED_OBS_COUNT	Number of Unauthorized observations in the observation bundle involved in this violation.
UNAUDITED_OBS_COUNT	Number of unaudited observations in the observation bundle involved in this violation.
RULE_NAME	Rule Name this violation is against.
COMPLIANCE_STANDARD_NAME	Compliance Standard Name this violation is against.
TARGET	Target Name this violation is against.

View: mgmt\$compliant_targets

Description: This view returns all evaluation and violation details for all targets. This is the same data that is shown in the Compliance Summary dashboard regions for targets.

Fields:

Field	Description
TARGET_ID	Internal representation of the Target
TARGET_NAME	Name of the Target
TARGET_TYPE	Target Type of the Target
TARGET_TYPE_INAME	Internal representation of the Target Type
CRIT_EVALS	Number of Critical-level Evaluations
WARN_EVALS	Number of Warning-level Evaluations
COMPLIANT_EVALS	Number of Compliant Evaluations
CRIT_VIOLATIONS	Number of Critical-level Violations
WARN_VIOLATIONS	Number of Warning-level Violations
MWARN_VIOLATIONS	Number of Minor Warning-level Violations
COMPLIANCE_SCORE	Current Compliance Score for the target

View: mgmt\$compliance_summary

Description: This view returns all evaluation and violation details for Compliance Standards and Frameworks. This is the same data that is shown in the Compliance Summary dashboard regions for Standards and Frameworks.

Fields:

Field	Description
ELEMENT_NAME	Display name of the Compliance Standard or Compliance Framework
ELEMENT_ID	Internal ID of the compliance standard or compliance framework
FRAMEWORK_ID	Internal ID of the Compliance Framework
CRIT_EVALS	Number of Critical-level Evaluations
WARN_EVALS	Number of Warning-level Evaluations
COMPLIANT_EVALS	Number of Compliant Evaluations
CRIT_VIOLATIONS	Number of Critical-level Violations
WARN_VIOLATIONS	Number of Warning-level Violations
MWARN_VIOLATIONS	Number of Minor Warning-level Violations
COMPLIANCE_SCORE	Current compliance score for the standard or framework
NON_COMPLIANT_SCORE	Current non-compliant score for the standard or framework
ELEMENT_TYPE	Type of element (1=Compliance Standard, 4=Compliance Framework)
AUTHOR	Author of the standard or framework
VERSION	Version of the standard or framework
ELEMENT_INAME	Internal representation of the standard or framework

View: mgmt\$compliance_trend

Description: This view returns the last 31 days compliance trend information for compliance frameworks and standards. This is the same data that is shown in the Compliance Summary dashboard trend regions for Standards and Frameworks.

Fields:

Field	Description
ELEMENT_ID	Internal ID representation of the standard or framework
FRAMEWORK_ID	Internal ID representation of the compliance framework
ELEMENT_NAME	Display name of the Compliance Standard or Compliance Framework
ELEMENT_INAME	Internal representation of the standard or framework
AVG_COMPLIANCE_SCORE	Average compliance score over last 31 days
DAILY_AVG_VIOLATIONS	Average number of violations per day over last 31 days
SNAPSHOT_TS	The snapshot timestamp
TOTAL_EVALS	Total evaluations over last 31 days

Field	Description
ELEMENT_TYPE	Type of element (1=Compliance Standard, 4=Compliance Framework)

29.11 Modifying Data Retention Periods

Real-time Monitoring features use partitioning and data retention configuration.

The following are the tables along with their default retention periods. When changing any retention periods, all tables related to Real-time monitoring must be changed to the same value to ensure that data is consistent across various features.

Note: For more information about modifying data retention values, see the chapter "Maintaining and Troubleshooting the Management Repository" in the book *Oracle Enterprise Manager Administration*.

Table Name	Default Retention Period
EM_CCC_WATCHDOG_ALERTS	366 Days
EM_CCC_HISTORY_JOBEXEC	366 Days
EM_CCC_OBSERVATION	366 Days
EM_CCC_OBSGROUP	366 Days
EM_CCC_OBS_GROUP_MAP	366 Days
EM_CCC_HISTORY_OBS_STATUS	366 Days
EM_CCC_HA_OBS	366 Days
BUNDLE_START_TIME	366 Days
BUNDLE_CLOSE_TIME	366 Days
BUNDLE_CLOSE_REASON	366 Days
EM_CCC_HA_OBSGROUP	366 Days
EM_CCC_FILEOBS_DIFF	366 Days
EM_CCC_AUTHOBS_CR_MAP	366 Days

29.12 Real-time Monitoring Supported Platforms

The following tables display the various platforms that support Real-time monitoring. For all tables, an X indicates support for the listed action and NS indicates "Not Supported".

The following Operating System platform combinations are not supported at this time:

- Microsoft Windows -- IA64
- Any Linux -- IA64, PA-RISC, POWER

Oracle Database Release 12 will not be supported until the version 12.1.0.4 Plug-in is released sometime after the Enterprise Manager 12.1.0.2 release.

29.12.1 OS User Monitoring

The following table displays the platforms that support OS User Monitoring.

Table 29–2 OS User Monitoring

Actions to Monitor	Oracle/Redhat Linux					Windows					
	V4		V5		V6	XP		2003 Server		2008 Server (R1 and R2)	
	X86 32 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 Bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit
Telnet Login (successful)	X	X	X	X	X	NS	NS	NS	NS	NS	NS
Telnet Logout (successful)	X	X	X	X	X	NS	NS	NS	NS	NS	NS
Telnet Login (failed)	X	X	X	X	X	NS	NS	NS	NS	NS	NS
SSH Login (successful)	X	X	X	X	X	NS	NS	NS	NS	NS	NS
SSH Logout (Successful)	X	X	X	X	X	NS	NS	NS	NS	NS	NS
SSH Login (failed)	X	X	X	X	X	NS	NS	NS	NS	NS	NS
Console Login (successful)	X	X	X	X	X	X	X	X	X	X	X
Console Logout (successful)	X	X	X	X	X	X	X	X	X	X	X
Console Login (failed)	X	X	X	X	X	X	X	X	X	X	X
FTP Login (successful)	NS	NS	NS	X	X	NS	NS	NS	NS	NS	NS
FTP Logout (successful)	NS	NS	NS	X	X	NS	NS	NS	NS	NS	NS
FTP Login (failed)	X	X	X	X	X	NS	NS	NS	NS	NS	NS
SU Login (successful)	X	X	X	X	X	NS	NS	NS	NS	NS	NS
SU Logout (successful)	X	X	X	X	X	NS	NS	NS	NS	NS	NS
SU Login (failed)	X	X	X	X	X	NS	NS	NS	NS	NS	NS
SUDO (successful)	X	X	X	X	X	NS	NS	NS	NS	NS	NS
SUDO (failed)	X	X	X	X	X	NS	NS	NS	NS	NS	NS
RDP Login (Successful)	NS	NS	NS	NS	NS	X	X	X	X	X	X
RDP Logout (Successful)	NS	NS	NS	NS	NS	X	X	X	X	X	X
RDP Login (failed)	NS	NS	NS	NS	NS	X	X	X	X	X	X

Table 29–3 OS User Monitoring

Actions to Monitor	SUSE Linux			Solaris				AIX			
	V10		V11	V9		V10	V11	V 5.3		V 6.1	
	X86 32 bit	X86 32 bit	X86 64 bit	X86 64 bit	Sparc	X86 64 bit	Sparc	X86 64 bit	Sparc	POWER	POWER
Telnet Login (successful)	X	X	X	X	X	X	X	X	X	X	X
Telnet Logout (successful)	X	X	X	X	X	X	X	X	X	X	X
Telnet Login (failed)	X	X	X	X	X	X	X	X	X	X	X

Table 29–3 (Cont.) OS User Monitoring

Actions to Monitor	SUSE Linux			Solaris				AIX			
	V10		V11	V9		V10	V11		V 5.3	V 6.1	
	X86 32 bit	X86 32 bit	X86 64 bit	X86 64 bit	Sparc	X86 64 bit	Sparc	X86 64 bit	Sparc	POWER	POWER
SSH Login (successful)	X	X	X	X	X	X	X	X	X	X	X
SSH Logout (Successful)	X	X	X	X	X	X	X	X	X	X	X
SSH Login (failed)	X	X	X	X	X	X	X	X	X	X	X
Console Login (successful)	NS	X	X	X	X	X	X	X	X	NS	NS
Console Logout (successful)	NS	X	X	X	X	X	X	X	X	NS	NS
Console Login (failed)	NS	X	X	X	X	X	X	X	X	NS	NS
FTP Login (successful)	X	NS	NS	X	X	X	X	X	X	X	X
FTP Logout (successful)	NS	NS	NS	X	X	X	X	X	X	X	X
FTP Login (failed)	X	X	X	X	X	X	X	X	X	X	X
SU Login (successful)	X	X	X	X	X	X	X	X	X	X	X
SU Logout (successful)	NS	X	X	NS	NS	NS	NS	X	X	NS	NS
SU Login (failed)	X	X	X	X	X	X	X	X	X	X	X
SUDO (successful)	X	X	X	NS	NS	NS	NS	NS	NS	NS	NS
SUDO (failed)	X	X	X	NS	NS	NS	NS	NS	NS	NS	NS
RDP Login (Successful)	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS
RDP Logout (Successful)	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS
RDP Login (failed)	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS

29.12.2 OS Process Monitoring

The following table displays the platforms that support OS User Monitoring.

Table 29–4 OS Process Monitoring

Actions to Monitor	Oracle/Redhat Linux					Windows					Solaris						
	V4		V5		V6	XP		2003 Server		2008 Server (R1 and R2)		V9		V10		V11	
	X86 32 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 64 bit	Sparc	X86 64 bit	Sparc	X86 64 bit	Sparc
Process Start (successful)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Process Stop (successful)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X

Table 29–5 OS Process Monitoring (continued)

Actions to Monitor	SUSE Linux			AIX	
	V10	V11		V5.3	V6.1
	X86 32 bit	X86 32 bit	X86 64 bit	POWER	POWER
Process Start (successful)	X	X	X	X	X
Process Stop (successful)	X	X	X	X	X

29.12.3 OS File Monitoring

For Linux v5, there are two possible ways monitoring can occur. Some actions to monitor below will work only on one or the other method. The two methods are to use the Loadable Kernel Module. Actions that are detectable ONLY with this method are annotated with “(KO)”. The other option is to not use the loadable kernel module, which will result in using the Linux built-in audited method. The actions that can only be monitored using this method are annotated with “(non-KO)”. The actions that have no annotation other than the check mark can be monitored using either approach.

Table 29–6 OS File Monitoring

Actions to Monitor	Linux			Windows						Solaris							
	V4		V5	V6		XP		2003 Server		2008 Server (R1 and R2)		V9		V10		V11	
	X86 32 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 64 bit	Spa rc	X86 64 bit	Spa rc	X86 64 bit	Spa rc
File Read (successful)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
File Delete (Successful)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
File Rename (successful)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
File Create (successful)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
File Content Modified (successful)	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
File Modified without content change	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
File Modified (failed)	NS	X (No n-KO)	NS	X (No n-KO)	X	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS
File Permission Change (successful)	NS	X (non-KO)	X (non-KO)	X (KO)	X	NS	NS	NS	NS	NS	NS	X	X	X	X	X	X
File Ownership Change (successful)	NS	X (non-KO)	X (non-KO)	X (KO)	X	NS	NS	NS	NS	NS	NS	X	X	X	X	X	X

Table 29–6 (Cont.) OS File Monitoring

Actions to Monitor	Linux			Windows						Solaris						
	V4	V5	V6	XP		2003 Server		2008 Server (R1 and R2)		V9	V10		V11			
	X86 32 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 64 bit	Spa rc	X86 64 bit	Spa rc	X86 64 bit	Spa rc	
File content modified (successful) Archive File	NS	X (non -KO)	X (non -KO)	X	X	X	X	X	X	X	X	X	X	X	X	X
File Read (failed)	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	NS	X	X	X	X	X
File Delete (failed)	NS	X (No n-K O)	X (No n-K O)	NS	NS	NS	NS	NS	NS	NS	NS	X	X	X	X	X
File Rename (failed)	NS	X (No n-K O)	X (No n-K O)	X (no n-K O)	NS	NS	NS	NS	NS	NS	NS	X	X	X	X	X
File Create (failed)	NS	X (non -KO)	X (non -KO)	X (no n-K O)	NS	NS	NS	NS	NS	NS	NS	X	X	X	X	X
File Permission Change (Failed)	NS	X (No n-K O)	X (No n-K O)	X (non -KO)	NS	NS	NS	NS	NS	NS	NS	X	X	X	X	X
File Ownership Change (failed)	NS	X (No n-K O)	X (No n-K O)	X (non -KO)	NS	NS	NS	NS	NS	NS	NS	X	X	X	X	X

Table 29–7 OS File Monitoring (continued)

Actions to Monitor	SUSE Linux			AIX	
	V10	V11		V5.3	V6.1
	X86 32 bit	X86 32 bit	X86 64 bit	POWER	POWER
File Read (successful)	X	X (KO)	X (KO)	X	X
File Delete (Successful)	X	X (KO)	X (KO)	X	X
File Rename (successful)	X	X	X	X	X
File Create (successful)	X	X	X	X	X
File Content Modified (successful)	X	X	X	X	X
File Modified without content change (successful)	X	X	X	X	X
File Modified (failed)	NS	NS	NS	X	X
File Permission Change (successful)	X	X (KO)	X	X	X
File Ownership Change (successful)	X	X (KO)	X	X	X
File content modified (successful) Archive File	X	X	X	X	X
File Read (failed)	NS	NS	NS	X	X
File Delete (failed)	NS	NS	NS	X	X

Table 29–7 (Cont.) OS File Monitoring (continued)

Actions to Monitor	SUSE Linux			AIX	
	V10	V11		V5.3	V6.1
	X86 32 bit	X86 32 bit	X86 64 bit	POWER	POWER
File Rename (failed)	NS	X (Non-KO)	X (Non-KO)	X	X
File Create (failed)	NS	NS	X (Non-KO)	X	X
File Permission Change (Failed)	NS	X (Non-KO)	X (Non-KO)	X	X
File Ownership Change (failed)	NS	X (Non-KO)	X (Non-KO)	X	X

29.12.4 OS Windows Registry Monitoring

The following table displays the platforms that support OS Windows Registry Monitoring.

Table 29–8 OS Windows Registry Monitoring

Actions to Monitor	Windows					
	XP		2003 Server		2008 Server (R1 and R2)	
	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit	X86 32 bit	X86 64 bit
Create Key (successful)	X	NS	X	X	X	X
Delete Key (successful)	X	NS	X	X	X	X
Create Value (successful)	X	NS	X	X	X	X
Modify Value (successful)	X	NS	X	X	X	X
Delete Value (successful)	X	NS	X	X	X	X
Create Key (failed)	X	NS	X	NS	NS	NS
Create Value (failed)	X	NS	X	NS	NS	NS
Modify Value (failed)	X	NS	X	NS	NS	NS
Delete value (failed)	X	NS	X	X	X	X

29.12.5 OS Windows Active Directory User Monitoring

The following table displays the platforms that support OS Windows Active Directory User Monitoring.

Table 29–9 OS Windows Active Directory User Monitoring

Actions to Monitor	Windows			
	2003 Server		2008 Server (R1 and R2)	
	X86 32 bit	X86 64 Bit	X86 32 bit	X86 64 bit
User Create (successful)	X	X	X	X
User Delete (successful)	X	X	X	X
User Attribute Modify (successful)	X	X	X	X

29.12.6 OS Windows Active Directory Computer Monitoring

The following table displays the platforms that support OS Windows Active Directory Computer Monitoring.

Table 29–10 OS Windows Active Directory Computer Monitoring

Actions to Monitor	Windows			
	2003 Server		2008 Server (R1 and R2)	
	X86 32 bit	X86 64 Bit	X86 32 bit	X86 64 bit
Computer Create (successful)	X	X	X	X
Computer Delete (successful)	X	X	X	X
Computer Attribute Modify (successful)	X	X	X	X

29.12.7 OS Windows Active Directory Group Monitoring

The following table displays the platforms that support OS Windows Active Directory Group Monitoring.

Table 29–11 OS Windows Active Directory Group Monitoring

Actions to Monitor	Windows			
	2003 Server		2008 Server (R1 and R2)	
	X86 32 bit	X86 64 Bit	X86 32 bit	X86 64 bit
Group Create (successful)	X	X	X	X
Group Delete (successful)	X	X	X	X
Group Attribute Modify (successful)	X	X	X	X
Group Member Add (successful)	X	X	X	X
Group Member Delete (successful)	X	X	X	X

29.12.8 Oracle Database Table Monitoring

The following table displays the platforms that support Oracle Database Table Monitoring.

Table 29–12 Oracle Database Table Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Insert (successful)	X	X	X	X
Select (successful)	X	X	X	X
Update (successful)	X	X	X	X
Delete (successful)	X	X	X	X
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Truncate (successful)	X	X	X	X
Alter (successful)	X	X	X	X
Comment (successful)	X	X	X	X
Rename (successful)	X	X	X	X
Lock (successful)	X	X	X	X
Grant (successful)	X	X	X	X
Revoke (successful)	X	X	X	X
Audit (successful)	X	X	X	X
NOAUDIT usage	X	X	X	X
Flashback (successful)		X	X	X

29.12.9 Oracle Database View Monitoring

The following table displays the platforms that support Oracle Database View Monitoring.

Table 29–13 Oracle Database View Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Insert (successful)	X	X	X	X
Select (successful)	X	X	X	X
Update (successful)	X	X	X	X
Delete (successful)	X	X	X	X
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Comment (successful)	X	X	X	X
Rename (successful)	X	X	X	X
Lock (successful)	X	X	X	X
Grant (successful)	X	X	X	X
Revoke (successful)	X	X	X	X
Audit (successful)	X	X	X	X
NOAUDIT usage	X	X	X	X
Flashback (successful)		X	X	X

29.12.10 Oracle Database Materialized View Monitoring

The following table displays the platforms that support Oracle Database Materialized View Monitoring.

Table 29–14 Oracle Database Materialized View Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Insert (successful)	X	X	X	X
Select (successful)	X	X	X	X
Update (successful)	X	X	X	X
Delete (successful)	X	X	X	X
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Alter (successful)	X	X	X	X
Comment (successful)	X	X	X	X
Lock (successful)	X	X	X	X
Grant (successful)	X	X	X	X
Revoke (successful)	X	X	X	X
Audit (successful)	X	X	X	X
NOAUDIT usage	X	X	X	X

29.12.11 Oracle Database Index Monitoring

The following table displays the platforms that support Oracle Database Index Monitoring.

Table 29–15 Oracle Database Index Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Alter (successful)	X	X	X	X
Analyze (successful)	NS	X	X	X

29.12.12 Oracle Database Sequence Monitoring

The following table displays the platforms that support Oracle Database Sequence Monitoring.

Table 29–16 Oracle Database Sequence Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Alter (successful)	X	X	X	X
Select (successful)	X	X	X	X
Grant (successful)	X	X	X	X
Revoke (successful)	X	X	X	X
Audit (successful)	X	X	X	X
NOAUDIT usage	X	X	X	X

29.12.13 Oracle Database Procedure Monitoring

The following table displays the platforms that support Oracle Database Procedure Monitoring.

Table 29–17 Oracle Database Procedure Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Execute (successful)	X	X	X	X
Grant (successful)	X	X	X	X
Revoke (successful)	X	X	X	X
Audit (successful)	X	X	X	X
NOAUDIT usage	X	X	X	X

29.12.14 Oracle Database Function Monitoring

The following table displays the platforms that support Oracle Database Function Monitoring.

Table 29–18 Oracle Database Function Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Execute (successful)	X	X	X	X
Grant (successful)	X	X	X	X
Revoke (successful)	X	X	X	X
Audit (successful)	X	X	X	X
NOAUDIT usage	X	X	X	X

29.12.15 Oracle Database Package Monitoring

The following table displays the platforms that support Oracle Database Package Monitoring.

Table 29–19 Oracle Database Package Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Execute (successful)	X	X	X	X
Grant (successful)	X	X	X	X
Revoke (successful)	X	X	X	X
Audit (successful)	X	X	X	X
NOAUDIT usage	X	X	X	X

29.12.16 Oracle Database Library Monitoring

The following table displays the platforms that support Oracle Database Library Monitoring.

Table 29–20 Oracle Database Library Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Execute (successful)	X	X	X	X
Grant (successful)	X	X	X	X
Revoke (successful)	X	X	X	X

29.12.17 Oracle Database Trigger Monitoring

The following table displays the platforms that support Oracle Database Trigger Monitoring.

Table 29–21 Oracle Database Trigger Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X

29.12.18 Oracle Database Tablespace Monitoring

The following table displays the platforms that support Oracle Database Tablespace Monitoring.

Table 29–22 Oracle Database Tablespace Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Alter (successful)	X	X	X	X

29.12.19 Oracle Database Cluster Monitoring

The following table displays the platforms that support Oracle Database Cluster Monitoring.

Table 29–23 Oracle Database Cluster Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Alter (successful)	X	X	X	X
Truncate (successful)	X	X	X	X

29.12.20 Oracle Database Link Monitoring

The following table displays the platforms that support Oracle Database Link Monitoring.

Table 29–24 Oracle Database Link Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X

29.12.21 Oracle Database Dimension Monitoring

The following table displays the platforms that support Oracle Database Dimension Monitoring.

Table 29–25 Oracle Database Dimension Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Alter (successful)	X	X	X	X

29.12.22 Oracle Database Profile Monitoring

The following table displays the platforms that support Oracle Database Profile Monitoring.

Table 29–26 Oracle Database Profile Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Alter (successful)	X	X	X	X

29.12.23 Oracle Database Public Link Monitoring

The following table displays the platforms that support Oracle Database Public Link Monitoring.

Table 29–27 Oracle Database Public Link Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X

29.12.24 Oracle Database Public Synonym Monitoring

The following table displays the platforms that support Oracle Database Public Synonym Monitoring.

Table 29–28 Oracle Database Public Synonym Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X

29.12.25 Oracle Database Synonym Monitoring

The following table displays the platforms that support Oracle Database Synonym Monitoring.

Table 29–29 Oracle Database Synonym Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Drop (successful)	X	X	X	X

29.12.26 Oracle Database Type Monitoring

The following table displays the platforms that support Oracle Database Type Monitoring.

Table 29–30 Oracle Database Type Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Create Type Body (successful)	X	X	X	X
Drop (successful)	X	X	X	X
Alter (successful)	X	X	X	X
Drop Type Body (successful)	X	X	X	X
Grant (successful)	X	X	X	X
Revoke (successful)	X	X	X	X
Audit (successful)	X	X	X	X
NOAUDIT usage	X	X	X	X

29.12.27 Oracle Database Role Monitoring

The following table displays the platforms that support Oracle Database Role Monitoring.

Table 29–31 Oracle Database Role Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Alter (successful)	X	X	X	X
Drop Type Body (successful)	X	X	X	X
Set (successful)	X	X	X	X

29.12.28 Oracle Database User Monitoring

The following table displays the platforms that support Oracle Database User Monitoring.

Table 29–32 Oracle Database User Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Create (successful)	X	X	X	X
Logon (successful)	X	X	X	X
Drop (successful)	X	X	X	X

Table 29–32 (Cont.) Oracle Database User Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
Alter (successful)	X	X	X	X
Logoff	X	X	X	X
Grant Role (successful)	X	X	X	X
Revoke Role (successful)	X	X	X	X
System Grant (successful)	X	X	X	X
System Revoke (successful)	X	X	X	X

29.12.29 Oracle Database SQL Query Statement Monitoring

The following table displays the platforms that support Oracle Database SQL Query Statement Monitoring.

Table 29–33 Oracle Database SQL Query Statement Monitoring

Actions to Monitor	Oracle Database			
	9i	10g	11g	12g
SQL Query Output Changed	X	X	X	X

Part IX

Oracle Site Guard

This part contains the following chapters:

- [Chapter 30, "Using Oracle Site Guard"](#)
- [Chapter 31, "Example Scenario: Using Oracle Site Guard"](#)

Using Oracle Site Guard

This chapter describes how to set up Oracle Site Guard for your existing Oracle Fusion Middleware disaster recovery solution, to perform operations like switchover and failover on the primary site and the standby site.

It contains the following topics:

- [Section 30.1, "New Features of Oracle Site Guard in Enterprise Manager Cloud Control 12c Release 2"](#)
- [Section 30.2, "Important Notes Before You Begin"](#)
- [Section 30.3, "Overview of Oracle Site Guard"](#)
- [Section 30.4, "Terminology Used in Oracle Site Guard"](#)
- [Section 30.5, "Using Oracle Site Guard: Task Overview"](#)
- [Section 30.6, "Installing Oracle Site Guard"](#)
- [Section 30.7, "Prerequisites for Configuring Oracle Fusion Middleware Products for Oracle Site Guard"](#)
- [Section 30.8, "Configuring Oracle Site Guard"](#)
- [Section 30.9, "Executing Oracle Site Guard Operations"](#)
- [Section 30.10, "Error Management Framework"](#)
- [Section 30.11, "Managing a Site Using Oracle Site Guard"](#)

30.1 New Features of Oracle Site Guard in Enterprise Manager Cloud Control 12c Release 2

This section provides an overview of the new features available in Oracle Site Guard in Enterprise Manager Cloud Control 12c Release 2 (Fusion Middleware plug-in release 12.1.0.3).

- [User Interface for Creating Oracle Site Guard Configuration](#)
- [Preferred Credential Support](#)
- [Re-Order Execution Order](#)

30.1.1 User Interface for Creating Oracle Site Guard Configuration

You can use the Enterprise Manager Cloud Control Console user interface to perform the following tasks:

- [Define Sites](#)

- Associate Credentials for Site
- Associate Pre-Scripts and Post-Scripts
- Associate Storage Scripts

For more information, see ["Configuring Oracle Site Guard"](#).

30.1.2 Preferred Credential Support

In this release, you can use named credentials or preferred credentials to run an operation plan.

Preferred credentials are used to simplify access to managed targets by storing target login credentials in the Management Repository. With preferred credentials set, users can access an Enterprise Manager target that recognizes those credentials, without being prompted to log in to the target. Preferred credentials are set on a per-user basis, thus ensuring the security of the managed enterprise environment.

- **Default Credentials:** Default credentials can be set for a particular target type, and will be available for all the targets of the target type. It will be overridden by target preferred credentials.
- **Target Credentials:** Target credentials are preferred credentials set for a particular target. They could be used by applications such as the job system, notifications, or patching. For example, if the user chooses to use preferred credentials while submitting a job, then the preferred credentials set for the target (target credentials) will be used. If the target credentials are not present, the default credentials (for the target type) will be used. If the default credentials are not present, the job will fail. If not specified, by default, preferred credentials refer to preferred target credentials.

For more information about setting up preferred credentials, see ["Setting Preferred Credential Using EMCLI Commands"](#).

30.1.3 Re-Order Execution Order

For more information, see ["Changing Execution Orders"](#).

30.2 Important Notes Before You Begin

Read the following notes before you start configuring Oracle Site Guard for Oracle Fusion Middleware components:

- Read "Terminology" in the *Oracle Fusion Middleware Disaster Recovery Guide* to understand the disaster recovery and Oracle Site Guard terminology used in this chapter.
- Read "Recommendations for Fusion Middleware Components" in the *Oracle Fusion Middleware Disaster Recovery Guide* before you configure Oracle Site Guard for Oracle Fusion Middleware.

Ensure that the disaster recovery environment is set up according to Oracle-recommended guidelines. For more information, see the following sections in the *Oracle Fusion Middleware Disaster Recovery Guide*:

- Ensure that host names are configured, as described in "Planning Host Names" in the *Oracle Fusion Middleware Disaster Recovery Guide*.

- Ensure that virtual IP addresses and virtual host names are configured, as described in "Virtual IP and Virtual Hostname Considerations" in the *Oracle Fusion Middleware Disaster Recovery Guide*.
- Read "Storage Considerations" in the *Oracle Fusion Middleware Disaster Recovery Guide*.
- Read "Database Considerations" in the *Oracle Fusion Middleware Disaster Recovery Guide*.
- Ensure that you have configured Oracle Data Guard to provide disaster recovery for Oracle Database, as described in "Database Considerations" in the *Oracle Fusion Middleware Disaster Recovery Guide*.

Note: Oracle Site Guard requires a database to be set up using Oracle Data Guard Broker. If Oracle Databases in a site are protected by Oracle Data Guard, you must configure Oracle Data Guard Broker for Oracle Data Guard, as described in the *Oracle Data Guard Broker* guide.

- Ensure that you have an existing Oracle Fusion Middleware disaster recovery setup, as described in "Setting Up and Managing Disaster Recovery Sites" in the *Oracle Fusion Middleware Disaster Recovery Guide*.

30.3 Overview of Oracle Site Guard

Oracle Site Guard primarily orchestrates switchover and failover between two disaster recovery sites. These sites should be created, as described in this chapter. Oracle Site Guard offers the following features:

- Ensures high availability, data protection, and disaster recovery for enterprise data.
- Performs Oracle Site Guard operations like switchover and failover. If the primary site becomes unavailable due to a planned or an unplanned outage, a Switchover or Failover process needs to be initiated using Oracle Site Guard.

This section includes the following topics:

- [Benefits of Oracle Site Guard](#)
- [Oracle Site Guard Operations](#)
- [Site Representation in Enterprise Manager Cloud Control](#)

30.3.1 Benefits of Oracle Site Guard

Oracle Site Guard provides the following benefits:

Reduction of Errors Due to Prepared Responses

Oracle Site Guard helps in reducing the possibility of human error in case of disasters. The recovery strategies are mapped out, tested, and rehearsed in prepared responses within the application. After starting an Oracle Site Guard operation for disaster recovery, human intervention is not required.

Storage Integration

Oracle Site Guard provides an easy mechanism to integrate with any storage. It integrates with storage appliances to perform switchover or failover, by using callouts to any user-specified storage role reversal scripts in the operation workflow.

Target Dependencies

Oracle Site Guard automatically handles dependencies between the targets while starting or stopping a site.

End-to-End Disaster Recovery Automation

Oracle Site Guard provides an end-to-end orchestration of the Oracle Site Guard operations by loosely integrating with storage appliances, to perform storage role reversals. It simultaneously integrates with Oracle Data Guard Broker to perform database role reversals. Oracle Site Guard then shuts down the primary site before performing disaster recovery operations like switchover or failover and brings up the standby site after the Oracle Site Guard operation is completed.

After Oracle Site Guard is configured, it manages all components in an application during an operation such as failover and switchover, and ensures that these operations are complete.

30.3.2 Oracle Site Guard Operations

Oracle Site Guard ensures high availability, data protection, and disaster recovery for Oracle Fusion Middleware 11g. It automates the following Oracle Site Guard operations:

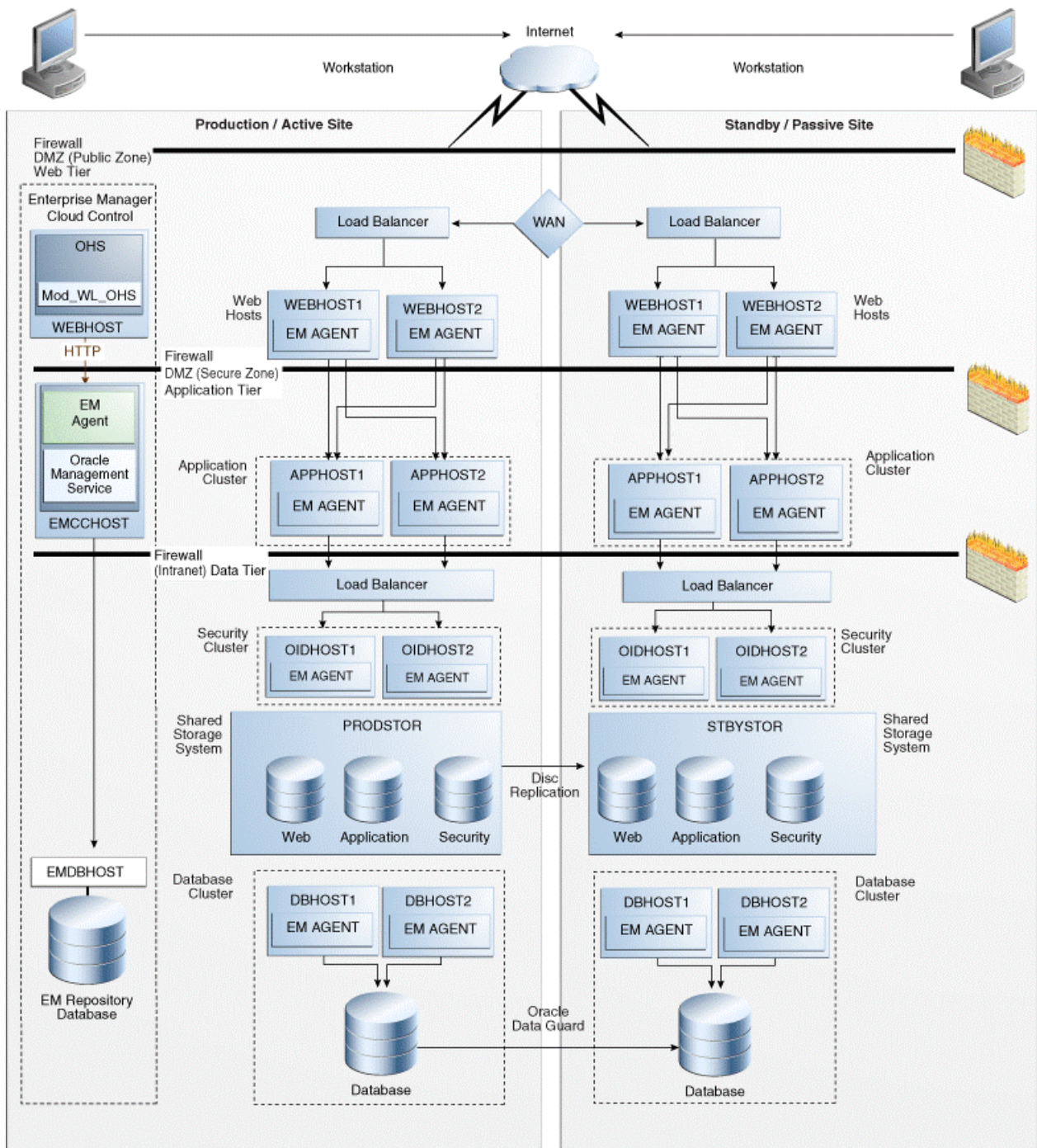
- Stopping a site
- Starting a site
- Site Switchover
- Site Failover

30.3.3 Site Representation in Enterprise Manager Cloud Control

A site is a collection of related targets in a data center. Oracle Site Guard performs operations like start-site, stop-site, switchover, and failover, on the site. It is required to run a group of applications simultaneously. For example, a site could consist of Oracle Fusion Middleware instances, databases, and storage devices. Oracle Site Guard uses the Enterprise Manager Cloud Control generic system target to represent a site. Every site, whether primary or standby, is represented as a generic system, which is a collection of other target types, such as Oracle Database and Oracle Fusion Middleware Domain. Oracle Site Guard only supports Enterprise Manager deployments where both primary and standby sites are managed by a single Enterprise Manager Cloud Control instance.

[Figure 30–1](#) shows an overview of an Oracle Fusion Middleware Disaster Recovery topology managed by a single Enterprise Manager Cloud Control instance.

Figure 30–1 Primary and Standby Site for Oracle Fusion Middleware Disaster Recovery Topology Managed by Enterprise Manager Cloud Control



The following are the key aspects of the topology in [Figure 30–1](#):

- A single Enterprise Manager Cloud Control instance monitors the primary site and the standby site.

- Oracle Management Agent (EM Agent) is installed on all hosts in the primary site and the standby site. For example:
 - OPMN managed system components (WEBHOST1 and WEBHOST2)
 - Oracle Fusion Middleware Applications (APPHOST1 and APPHOST2)
 - Oracle RAC Database (DBHOST1 and DBHOST2)

Oracle Management Agent (EM Agent) is one of the core components of Enterprise Manager Cloud Control that enables you to convert an unmanaged host to a managed host in the Enterprise Manager system. The Management Agent works in conjunction with the plug-ins to manage the targets running on that managed host.

- When there is a failure or planned outage of the primary site, Oracle Site Guard automates the following steps to enable the standby site to assume the production role in the topology:
 1. Stops services and applications running on the primary site, and unmounts the storage on the primary site.
 2. Stops the replication from the primary site to the standby site (when a failure occurs, replication stops due to the failure), and performs storage role reversal.
 3. Performs a failover or switchover of the Oracle Databases using Oracle Data Guard Broker.
 4. Mounts the storage on the standby site.
 5. Starts the services and applications on the standby site, and assumes the production role.

Note: If continuous replication is not configured, Oracle recommends that you create a final replication between the primary and the standby sites, before the storage switchover.

30.4 Terminology Used in Oracle Site Guard

The following terms are used throughout this chapter when discussing about Oracle Site Guard:

- Site

A site is a set of different targets in a datacenter needed to run a group of applications. For example, a site could consist of Oracle Fusion Middleware instances, databases, storage, and so on. A datacenter may have more than one site defined by Oracle Site Guard and each of them managed independently for operations like switchover and failover.
- Site Failover

The process of making the current standby site the new primary site after the primary site becomes unexpectedly unavailable (for example, due to a disaster at the primary site). This book also uses the term "failover" to refer to a site failover.
- Site Switchover

The process of reversing the roles of the primary site and standby site. Switchovers are planned operations done for periodic validation or to perform planned maintenance on the current primary site. During a switchover, the current standby site becomes the new primary site, and the current primary site

becomes the new standby site. This book also uses the term "switchover" to refer to a site switchover.

- Oracle Site Guard Configuration

An Oracle Site Guard configuration contains settings such as, site creation, pre-scripts or post-scripts, storage, and credentials that are applicable to its operations.

- Target

Targets are core Enterprise Manager entities which represent the infrastructure and business components in an enterprise. These components need to be monitored and managed for efficient functioning of the business. For example, Oracle Fusion Middleware farm or Oracle Database.

- Generic System

A System is the set of targets (hosts, databases, application servers, and so on) that work together to host your applications. To monitor an application in Enterprise Manger, you would first create a System, that consists of the database, listener, application server, and hosts targets on which the applications run.

- Operation Plan

An operation plan contains the flow of execution for a particular Oracle Site Guard operation. It defines the order in which the steps of an operation plan should be executed, in addition to other attributes, such as, serial, parallelism, and so on.

30.5 Using Oracle Site Guard: Task Overview

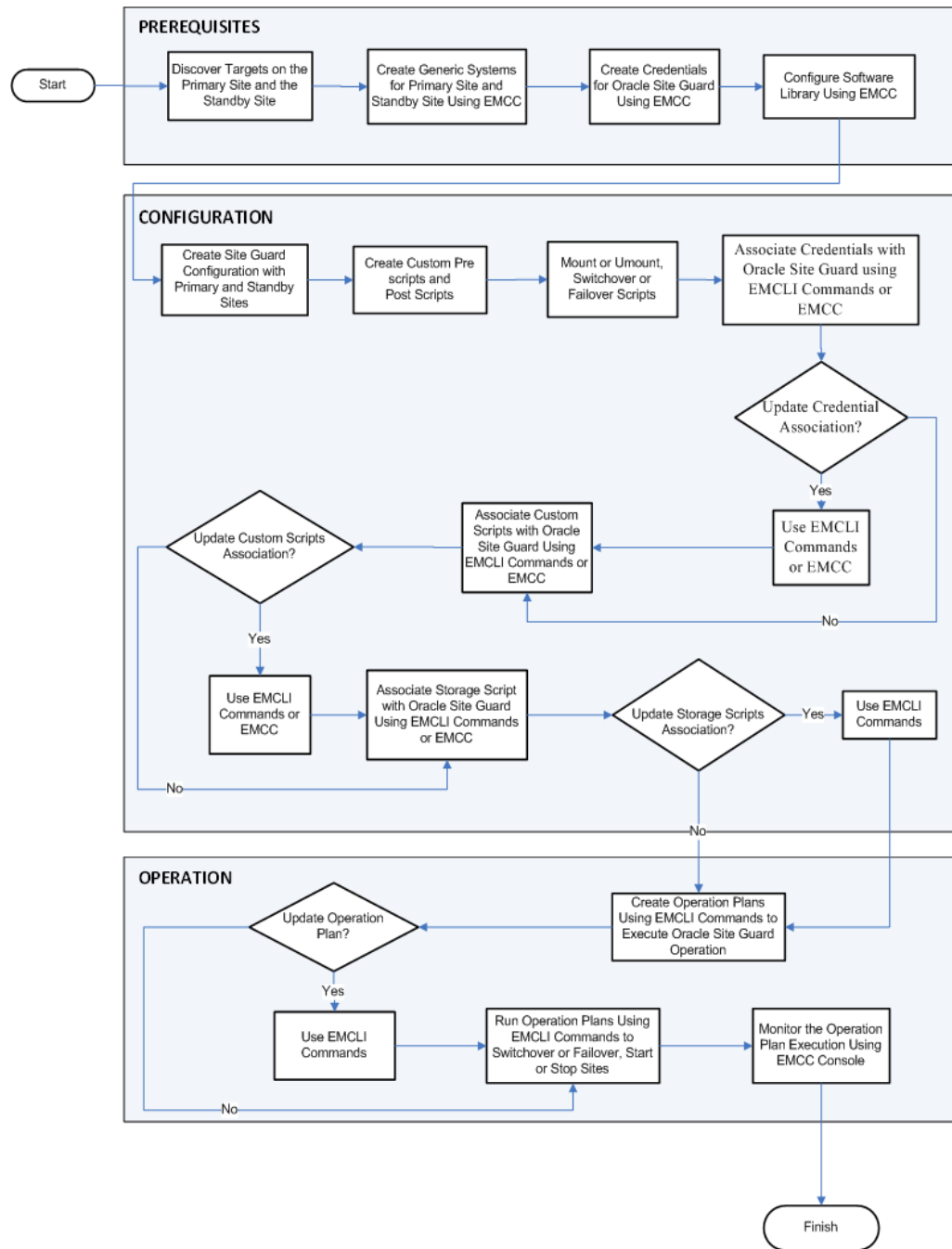
This section briefly describes how to use Oracle Site Guard to orchestrate switchover or failover operations between two sites. It contains the following topics:

- [Task Overview](#)
- [Task Roadmap](#)

30.5.1 Task Overview

[Figure 30–2](#) shows a flow chart of the tasks that you need to perform while using Oracle Site Guard for switchover or failover operations.

Figure 30–2 Task Overview of Oracle Site Guard



30.5.2 Task Roadmap

Table 30–1 describes each of the steps in the task-overview flow chart, which is shown in Figure 30–2. The table also provides pointers for to get more information about each of the task in the process.

Table 30–1 Table Describing the Steps for Using Oracle Site Guard

Task	Description	More Information
Discover targets on the primary site and the standby site	The <i>Oracle Enterprise Manager Cloud Control Administrator's Guide</i> guide provides a high-level overview of how to discover targets on a primary site.	Discovering Targets on the Primary Site and the Standby Site
Create generic systems for primary site and standby site using EMCC	Oracle Site Guard uses the Enterprise Manager Cloud Control generic system target to represent a site. Oracle Site Guard only supports Enterprise Manager deployments where both primary and standby sites are managed by single Enterprise Manager Cloud Control.	Creating Generic Systems for the Primary and Standby Sites
Create credentials for Oracle Site Guard using EMCC	Create named and preferred credentials before associating them with the Oracle Site Guard configuration.	Creating Credentials
Configure software library using EMCC	Oracle Software Library (Software Library) is a repository that stores scripts that Oracle Site Guard requires, to execute the operation plan. Configuring Oracle Software Library is a one-time process.	Configuring the Software Library
Configure Oracle Site Guard on primary sites and standby sites	You need to create pre-scripts, post-scripts, and storage scripts before configuring Oracle Site Guard on primary sites and standby sites.	Configuring Oracle Site Guard
Create custom pre scripts and post scripts	Custom scripts (pre-scripts and post-scripts) can be created and executed at the site level, for a given Oracle Site Guard operation. This is an optional configuration.	Creating Pre-Scripts and Post-Scripts
Create storage mount or unmount, or switchover or failover scripts	Create storage scripts (mount, unmount, switchover, failover) to manage storage-related tasks during switchover and failover operations.	Creating Storage Scripts
Associate credentials with Oracle Site Guard using EMCLI commands or EMCC	After you create named and preferred credentials, ensure that you associate them with the Oracle Site Guard configuration.	<ul style="list-style-type: none"> ■ Associating Credentials Using Enterprise Manager Cloud Control Console ■ Associating Credentials Using EMCLI Commands
Update credential association	After you associate credentials with Oracle Site Guard configuration, you can update them later, as required.	Associating Credentials

Table 30–1 (Cont.) Table Describing the Steps for Using Oracle Site Guard

Task	Description	More Information
Associate custom scripts with Oracle Site Guard using EMCLI commands or EMCC	If you need to execute one or more custom scripts (pre-scripts and post-scripts) as part of a Oracle Site Guard operation workflow, ensure that you associate it with the Oracle Site Guard configuration.	Associating Pre-Scripts and Post-Scripts
Update custom scripts association	After you associate custom scripts with the Oracle Site Guard configuration, you can update them later, as required.	<ul style="list-style-type: none"> ▪ Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console ▪ Associating Pre-Scripts and Post-Scripts Using EMCLI Commands
Associate storage script with Oracle Site Guard using EMCLI commands or EMCC	The storage scripts (mount, unmount, switchover, failover) need to be associated with Oracle Site Guard configuration. These scripts are then executed at designated points in the Oracle Site Guard switchover or failover workflow.	<ul style="list-style-type: none"> ▪ Associating Storage Scripts Using Enterprise Manager Cloud Control Console ▪ Associating Storage Scripts Using EMCLI Commands
Update storage scripts association	After you associate storage scripts with Oracle Site Guard configuration, you can update them later, as required.	<ul style="list-style-type: none"> ▪ Associating Storage Scripts Using Enterprise Manager Cloud Control Console ▪ Associating Storage Scripts Using EMCLI Commands
Create operation plans using EMCLI commands, to execute Oracle Site Guard operation	An operation plan contains the execution flow for the Oracle Site Guard operation. You can either use the default operation plan or update it to change the order of targets within their corresponding steps.	Creating an Operation Plan
Run operation plans using EMCLI commands to switchover or failover, or to start or stop sites	After an operation plan is created for a particular operation type, you can execute it when required, to perform the corresponding operation.	<ul style="list-style-type: none"> ▪ Stopping a Site ▪ Starting a Site ▪ Performing Site Switchover ▪ Performing Site Failover
Monitor the operation plan execution using EMCC console	After executing an operation plan, you can monitor its status using the EMCC console.	Monitoring an Operation Plan

30.6 Installing Oracle Site Guard

Oracle Site Guard is included with Enterprise Manager Cloud Control 12c Release 1 (12.1.0.3). You can manage an Oracle Site Guard configuration by using Enterprise Manager command-line interface (EMCLI) or console. To install Oracle Site Guard, complete the following steps:

Note: For information about Oracle Site Guard licensing, see *Oracle Enterprise Manager Licensing Information*.

- Install Enterprise Manager Cloud Control 12c Release 1 (12.1.0.3) for your existing Oracle Fusion Middleware enterprise deployment. For information about installing Enterprise Manager Cloud Control 12 c Release 1 (12.1.0.3), see "*Oracle Enterprise Manager Cloud Control Basic Installation Guide*."

Note: Ensure that you install Oracle Management Agent (EM Agent) on each of the hosts managed by Enterprise Manager, as described in the chapter "Installing Oracle Management Agent" in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

- Install the Enterprise Manager Command-Line Interface (EMCLI), as described in the chapter "Command Line Interface Concepts and Installation" in the *Oracle Enterprise Manager Command Line Interface Guide*.

Note: Oracle recommends that you install EM CLI in the same Middleware home where Oracle Management Service is installed. For example, `OMS_HOME/bin/emcli`.

30.7 Prerequisites for Configuring Oracle Fusion Middleware Products for Oracle Site Guard

The following are the prerequisites for configuring Oracle Fusion Middleware 11g products for Oracle Site Guard:

- [Discovering Targets on the Primary Site and the Standby Site](#)
- [Creating Generic Systems for the Primary and Standby Sites](#)
- [Creating Credentials](#)
- [Configuring the Software Library](#)

30.7.1 Discovering Targets on the Primary Site and the Standby Site

For information about discovering targets on the primary site, see "Adding Targets" in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Oracle Site Guard supports discovery of the following target types:

- Oracle Fusion Middleware farm
- Oracle Fusion Middleware managed system components, such as Oracle HTTP Server and Oracle Internet Directory (part of the Oracle Fusion Middleware farm)
- Real Application Cluster (RAC) databases
- Single instance database

For a two-site deployment, the targets in the primary site should be discovered first, followed by the targets in the standby site.

A site should be up for its targets to be discovered. For a two-site deployment, you must first discover the targets in the primary site. Once you discover the targets in the

primary site, you must manually perform a switchover operation, so that the standby site takes over the production role, as described in "Performing a Switchover" in *Oracle Fusion Middleware Disaster Recovery Guide*

After performing a switchover, you can discover the targets for the standby site by completing the steps described in "Adding Targets" in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Note: After you discover the targets for the standby site, you must manually perform a switchover operation, so that the primary site takes over the production role, as described in "Performing a Switchover" in *Oracle Fusion Middleware Disaster Recovery Guide*.

30.7.2 Creating Generic Systems for the Primary and Standby Sites

You must create a generic system for the primary site and the standby site. Each generic system must include all targets, Oracle Fusion Middleware farms and Databases, pertaining to the site that it represents.

Create the generic system using one of the following options:

- [Using Enterprise Manager Cloud Control Console to Create a Generic System](#)
- [Using EMCLI Commands to Create a Generic System](#)

30.7.2.1 Using Enterprise Manager Cloud Control Console to Create a Generic System

To create a generic system for the primary site, using an Enterprise Manager Cloud Control console, complete the following steps:

1. Log in to Enterprise Manager as an `EM_CLOUD_ADMINISTRATOR` user.
2. Select **Targets** and then select **Systems**.
The **Systems** page is displayed.
3. Select **Generic System** from the drop-down menu and click **Add**.
4. In the **General** section, enter the name for your primary system.
5. In the **Member** section, click **Add**.
6. Choose the targets, and click **Select**. You must associate the following:
 - Oracle Fusion Middleware Farm which includes:
 - Administration Server
 - Managed Servers
 - OPMN-managed system components
 - If you are using Oracle RAC Database then you must associate it with a **Cluster Database** target. For a single database instance, you must associate it with a **Database Instance** target.

Note: Ensure that the following target types are *not* added to the generic system:

- Database System
 - Individual RAC Database instances
-
-

7. Select the time zone from the drop-down menu.
8. Click **Next**.
The **Define Associations** page is displayed.
9. Click **Next**.
The **Availability Criteria** page is displayed.
10. From Availability Criteria, select the **Any Of The Key Members** option.
11. Select **AdminServer** in the **Members** pane and double-click.
The **AdminServer** is removed from the **Members** pane and added in the **Key Members** pane.
12. Click **Next**.
The **Charts** page is displayed.
13. Click **Next**.
The **Review** page is displayed.
14. Review your settings, and click **Finish**.

30.7.2.2 Using EMCLI Commands to Create a Generic System

Create a generic system by running the following `emcli` commands (located at `OMS_HOME/bin/emcli`) in the command-line interface:

Note: For information about setting up a new EMCLI client, see the Enterprise Manager Command-Line Interface Download page within the Cloud Control console. To access the page, in **Cloud Control**, from the **Setup** menu, click **Command Line Interface**.

```
emcli create_system
-name="name"
-type=system
-add_members="name1:type1;name2:type2;..."]...
-timezone_region="actual_timezone_region"
```

Note: To get status and alert information for targets, you can run `get_targets` command. For more information, see the chapter "Verb Reference" in the *Oracle Enterprise Manager Command Line Interface Guide*.

Parameter	Description
-name	Enter a name for the system.
-type	Enter <code>generic_system</code> as the type.
-add_members	Add existing targets to the system. Each target is specified as a name-value pair <code>target_name:target_type</code> . You can specify this option more than once.
-timezone_region	Specify the time zone region. The time zone you specify here is used for scheduling operations such as jobs and blackouts, on the system.

See "create_system" in the *Oracle Enterprise Manager Command Line Interface Guide*.

30.7.3 Creating Credentials

Create the credentials for the following targets associated with Oracle Site Guard, using Enterprise Manager Cloud Control Console:

- Host (for normal user)
- Host (users with root privileges)
- Oracle WebLogic Server
- Oracle Database

Oracle Site Guard supports the following credentials:

- Named Credentials
- Preferred Credentials

For more information, see "Preferred Credentials" in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Notes:

- The credentials created here are later associated with the Oracle Site Guard configuration. Oracle Site Guard supports specifying the same credentials for all targets of the same target type. For example, all databases in a system can have the same sysdba credentials. Oracle Site Guard also allows the targets of same kind to have different credentials.
 - If the credentials are the same across the nodes (primary and standby site), you need not create credentials for the targets running on the standby site.
-
-

Creating Named Credentials Using Enterprise Manager Cloud Control Console

To create a named credentials using Enterprise Manager Cloud Control Console, complete the following steps:

1. Log in to Enterprise Manager as an EM_CLOUD_ADMINISTRATOR user.
2. From the **Setup** menu, select **Security**, then select **Named Credentials**.

The **Named Credentials** page is displayed.

3. Click **Create**.

The **Create Credential** page is displayed.

4. In the **General Properties** section, specify the following:
 - **Credential name:** Enter a name for the credential.
 - **Credential description:** Enter the credential description.
 - **Authenticating Target Type/ Credential type/ Scope:** Enter the details as specified in the following table:

Element	Host Details	Host (root-User Privileges) Details	Oracle WebLogic Server	Database Instance
Authenticating Target Type	Host	Host	Oracle WebLogic Server	Database Instance
Credential type	Host Credentials	Host Credentials	Oracle WebLogic Credentials	Database Credentials
Scope	Global	Global	Global	Global

5. In the **Credential Properties** section, specify the following:

- **UserName:** Enter the username.
- **Password:** Enter the password.
- **Confirm Password:** Enter the password again.
- **Run Privilege/ Role:** Enter the details as specified in the following table:

Element	Host	Host (Users with root privileges)	Oracle WebLogic Server	Database Instance
Run Privilege	None	Select Sudo and enter values in the Run As fields	Oracle WebLogic Administration user credentials	Oracle Database SYS user credential
Role	None	None	None	SYSDBA

6. Click **Test and Save**. To test credentials, select the appropriate **Test Target Type** from the drop-down menu for which you want to test the credentials, and specify **Test Target Name**.

Creating Named Credentials Using EMCLI Commands

You can create a named credential by running the following emcli commands in the command-line interface:

```
emcli create_named_credential
  -cred_name="cred_name"
  -auth_target_type="auth_target_type"
  -cred_type="cred_type"
  -attributes="p1:v1;p2:v2"
```

Parameter	Description
cred_name	Sets the name for this credential set.
auth_target_type	Set the authenticating target type.
cred_type	Set the credential type for the target/credential set.

Parameter	Description
attributes	Enter the following credential column values: colname:colvalue;colname:colvalue You can change the value of the separator using -separator=attributes=newvalue. You can also change the value of the sub-separator using -subseparator=attributes=newvalue.

Setting Preferred Credential Using EMCLI Commands

You can set a named credential as a target-preferred credential by running the following `emcli` commands in the command-line interface:

Note: Oracle recommends that you to set the preferred credential using the `emcli` commands.

```
emcli set_preferred_credential
-set_name="set_name"
-target_name="target_name"
-target_type="type"
-credential_name="name"
[-credential_owner ="owner"]
```

Note: [] indicates that the parameter is optional.

Parameter	Description
set_name	Sets the preferred credential for this credential set.
target_name	Sets the preferred credential for this target.
target_type	Target type for the target/credential set.
credential_name	Name of the credential.
credential_owner	Owner of the credential. This defaults to the currently logged-in user.

Example:

```
emcli set_preferred_credential
-set_name="HostCredsNormal"
-target_name="test.example.com"
-target_type="host"
-credential_name="MyHostCredentials"
-credential_owner="Admin"
```

30.7.4 Configuring the Software Library

Oracle Software Library (Software Library) is a repository that stores scripts required by Oracle Site Guard to execute the operation plan. To configure the storage location for the Oracle Software Library, complete the following steps:

Note: Configuring Oracle Software Library is a one-time process. Enterprise Manager requires you to configure Oracle Software Library before proceeding with any deployment-procedure related tasks. Perform the steps listed in this section after confirming that Oracle Software Library is not configured.

1. Log in to Enterprise Manager as an `EM_CLOUD_ADMINISTRATOR` user.
2. From the **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.

The **Software Library: Administration** page is displayed.

3. Select **OMS Shared Filesystem** from the **Storage Type** drop-down box.
4. Click **Add**.
5. Specify a Name and Location that is accessible to all OMSs and click **OK**.

Note: As the storage location for the Software Library must be accessible to all OMSs as local directories, in a multi-OMS scenario, you must set up a clustered filesystem using OCFS2 or NFS. For single OMS systems, any local directory is sufficient.

A job is executed to upload all the out-of-box content.

Note: For more information, see "Configuring Software Library" in the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

30.8 Configuring Oracle Site Guard

This section describes the setup and configuration of Oracle Site Guard in Enterprise Manager Cloud Control to manage Oracle Fusion Middleware Disaster operations on the primary site and the standby site.

Ensure that you create the scripts that are needed to configure Oracle Site Guard:

- [Creating Pre-Scripts and Post-Scripts](#)
- [Creating Storage Scripts](#)

Creating Pre-Scripts and Post-Scripts

You can create custom scripts to be executed at the site level for the Oracle Site Guard operation (stop, start, switchover, or failover) workflow. Each script can be associated with more than one host in a site. You can create the following scripts:

- Pre-Script
- Post-Script

Create the required scripts and save them in a location of your choice on each of the hosts from where the script will be executed. After creating and testing the script, ensure that you associate the script with Oracle Site Guard, as described in "[Associating Pre-Scripts and Post-Scripts](#)".

Notes:

- A custom script should be a shell script and it must have clearly defined return codes. The script must return 0 on success, and non-zero values on failure.
 - Ensure that you have the required privilege to run the script.
-

Creating Storage Scripts

You can create the following storage scripts:

- Mount Script
- Unmount Script
- Switchover script
- Failover Script

Create the required scripts and save them to the location of your choice on each of the hosts from where the script will be executed. After creating and testing the script, you must associate that with Oracle Site Guard, as described in "[Associating Storage Scripts](#)".

Oracle Site Guard provides the following sample scripts for Sun ZFS and NetApp Storage appliances:

- `mount-unmount.sh`
- `switchoverStorage.sh`

The sample scripts are located in the `AGENT_HOME/plugins/oracle.sysman.emas.agent.plugin_12.1.0.3.0/scripts` directory after completing the Oracle Management Agent (EM Agent) installation.

Notes: After running the script, verify that the execution return code value is 0. If you get any other value for the return code, then the script is considered to have failed. Ensure that you implement the script with the proper return code.

The following are examples of scripts Sun ZFS and NetApp Storage appliances:

- **mount-unmount.sh**

Run the following command to mount or unmount directories on the storage appliance:

```
./mount-unmount.sh [-t operation_type ] [-d directories_to_mount_or_unmount]
```

Note:

- If there are multiple directories to be mounted or unmounted on the appliance, use commas to separate the directories.
 - Ensure that the `/etc/fstab` file is updated with the devices that you want to mount or unmount.
-

For example,

To mount multiple directories, run the following command:

```
./mount-umount.sh [-t mount] [-d
/u02/oracle/config,/u02/oracle/product,/u02/oracle/stage]
```

To mount a single directory, run the following command:

```
./mount-umount.sh -t mount -d /u01/app/oracle/product/test
```

To unmount multiple directories, run the following command:

```
./mount-umount.sh [-t unmount] [-d
/u02/oracle/config,/u02/oracle/product,/u02/oracle/stage]
```

To unmount a single directory, run the following command:

```
./mount-umount.sh -t umount -d /u01/app/oracle/product/test
```

- **switchoverStorage.sh**

For Sun ZFS appliance:

Run the following command to switch over storage:

```
./switchoverStorage.sh -u appliance_user -h appliance -j project_name -p pool_
name -s sourceID
```

For example:

```
./switchoverStorage.sh -u root -h host.test.example.com -j SiteGuard -p pool-0
-s source-000
```

- **ntapstorage.pl**

Note: Oracle Site Guard currently supports only shell scripts. Create a sample shell script to invoke the perl script, `ntapstorage.pl`.

Ensure that the sample wrapper shell script invokes the `ntapstorage.pl` script for each pair of source and destination volumes. For example, if there are two pairs of source and destination volumes between the primary and standby sites, then this wrapper script should invoke `ntapstorage.pl` script twice.

Run the perl script `ntapstorage.pl`. Do the following:

- a. Call the perl script, `ntapstorage.pl`, from the following sample wrapper shell script:

```
#!/bin/bash
perl ntapstorage.pl $@
```

- b. Run the following command to switch over storage:

```
./sample-wrapper.sh -sm <sip1:sv1/dip1:dv1> <update break | resync | break
| release | break release | break release resync> [-ntap_src_user
<sip2:root/password> -ntap_dest_user <dip2:root/password> -encrypted
<true/false> ]
```

For example:

```
./sample-wrapper.sh -sm primary-storage:vol1/standby-storage:vol2 update
```

After creating the required scripts, complete the following steps to configure Oracle Site Guard:

- [Configuring Sites Using Generic Systems](#)
- [Associating Credentials](#)
- [Associating Pre-Scripts and Post-Scripts](#)
- [Associating Storage Scripts](#)

30.8.1 Configuring Sites Using Generic Systems

Configure the primary and standby sites using generic systems, and associate them with Oracle Site Guard.

You can add the configuration for the primary and standby sites using one of the following options:

- [Configuring Sites Using Enterprise Manager Cloud Control Console](#)
- [Configuring Sites Using EMCLI Commands](#)

30.8.1.1 Configuring Sites Using Enterprise Manager Cloud Control Console

To associate the standby system with the primary system, complete the following steps:

1. Log in to Enterprise Manager as an `EM_CLOUD_ADMINISTRATOR` user.
2. From the **Targets** menu, select **Systems**.
The **Systems** page is displayed.
3. Select the primary system (created in "[Creating Generic Systems for the Primary and Standby Sites](#)").
4. Click **Generic System > Site Guard > Configure**.
The **Site Guard Configuration** page is displayed.
5. In the **Standby System(s)** section, click **Add**.
The **Search and Select: Standby Systems** page is displayed.
6. Choose the standby system, and click **Select**.
7. Click **Save**.

30.8.1.2 Configuring Sites Using EMCLI Commands

To add the configuration for the primary and standby sites, you must run the following `emcli` commands in the command-line interface:

Note: For information about logging in to `emcli`, see chapter "Command Line Interface Concepts and Installation" in the *Oracle Enterprise Manager Command Line Interface Guide*.

```
emcli create_siteguard_configuration
      -primary_system_name="system_name"
      -standby_system_name="system_name"
```

Parameter	Description
-primary_system_name	Enter the name of your system, which is associated with the primary site.
-standby_system_name	Enter the name of your system, which is associated with the standby site.

To display information about the association between existing primary and standby sites, run the following `emcli` commands in the command-line interface:

```
emcli get_siteguard_configuration
      -primary_system_name="system_name"
      -standby_system_name="system_name"
```

30.8.2 Associating Credentials

You must associate credentials created in ["Creating Credentials"](#) with the targets in each site.

Associate the credentials for the following targets:

- Host, where Oracle Fusion Middleware and Oracle Database are installed and configured (for normal user and users with root privileges)
- Oracle WebLogic Administration Server
- Oracle Database

You can associate the credentials using one of the following options:

- [Associating Credentials Using Enterprise Manager Cloud Control Console](#)
- [Associating Credentials Using EMCLI Commands](#)

30.8.2.1 Associating Credentials Using Enterprise Manager Cloud Control Console

To associate the credentials for the primary site, complete the following steps:

1. Log in to Enterprise Manager as an `EM_CLOUD_ADMINISTRATOR` user.
2. Select **Targets** and then select **Systems**.
The **Systems** page is displayed.
3. Select the primary system (created in ["Creating Generic Systems for the Primary and Standby Sites"](#)).
4. Click **Generic System > Site Guard > Configure**.
The **Site Guard Configuration** page is displayed.
5. Click the **Credentials** tab.
6. In the **Normal Host Credentials** section, click **Add**.
The **Add Normal Host Credentials** page is displayed.
7. Enter the following details:
 - **Target:** Select the target name.
 - **Use Preferred Credentials:** If you are using preferred credentials, then select the checkbox.

- **Named Credential:** If you are using named credentials, then select the credential name.
- Click **Save**.
8. In the **Privileged Host Credentials** section, click **Add**.
The **Add Privileged Host Credentials** page is displayed.
 9. Enter the following details:
 - **Target:** Select the target name.
 - **Use Preferred Credentials:** If you are using preferred credentials, then select the checkbox.
 - **Named Credential:** If you are using named credentials, then select the credential name.Click **Save**.
 10. In the **Oracle WebLogic Administration Credentials** section, click **Add**.
The **Add Oracle WebLogic Administration Credentials** page is displayed.
 11. Enter the following details:
 - **Target:** Select the target name.
 - **Use Preferred Credentials:** If you are using preferred credentials, then select the checkbox.
 - **Named Credential:** If you are using named credentials, then select the credential name.Click **Save**.
 12. In the **Database Credentials** section, click **Add**.
The **Add Database Credentials** page is displayed.
 13. Enter the following details:
 - **Target:** Select the target name.
 - **Use Preferred Credentials:** If you are using preferred credentials, then select the checkbox.
 - **Named Credential:** If you are using named credentials, then select the credential name.Click **Save**.
 14. Choose the standby system, and click **Select**.
 15. Use the above steps to associate the credentials for the standby site.

30.8.2.2 Associating Credentials Using EMCLI Commands

Associate the credentials for the targets by running the credential framework `emcli` commands in the command-line interface:

```
emcli create_siteguard_credential_association
    -system_name="name"
    -credential_type="type"
    -credential_name="name"
    -credential_owner="owner"
    -use_preferred_credential="true or false"
```

Parameter	Description
-system_name	Specify the name of the system, which is associated with the site.
-credential_type	Specify the credential type depending on the target: Host: HostNormal Host (users with root privileges): HostPrivileged Oracle WebLogic Server: WLSAdmin Oracle Database: DatabaseSysdba
-credential_name	Specify a name for the credential.
-credential_owner	Specify the owner of the credential.
-use_preferred_credential	If you are using Preferred Credentials, then specify true.

30.8.3 Associating Pre-Scripts and Post-Scripts

You can associate pre-scripts or post-scripts (created in "[Creating Pre-Scripts and Post-Scripts](#)") for the Oracle Site Guard operation workflow.

Note: You can specify the script arguments as name-value pairs with the script. For example, `test.sh -param1 value1 -param2 value2`.

You can associate pre-scripts and post-scripts using one of the following options:

- [Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console](#)
- [Associating Pre-Scripts and Post-Scripts Using EMCLI Commands](#)

30.8.3.1 Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console

To associate pre-scripts and post-scripts for the primary site, complete the following steps:

1. Log in to Enterprise Manager as an `EM_CLOUD_ADMINISTRATOR` user.
2. Select **Targets** and then select **Systems**.
The **Systems** page is displayed.
3. Select the primary system (created in "[Creating Generic Systems for the Primary and Standby Sites](#)").
4. Click **Generic System > Site Guard > Configure**.
The **Site Guard Configuration** page is displayed.
5. Click the **Pre/Post Scripts** tab.
6. Click **Add**.
The **Add Pre/Post Scripts** page is displayed.
7. Enter the following details:
 - **Script Path:** Enter the path to the script, or click the search icon and specify the path to the script.
 - **Target Hosts:** Select the target name.

- **Script Type:** The type of script, depending on the function you want to perform, select one of the following options:
 - **Pre-Script**
 - **Post-Script**
- **Operation Type:** The function of the operation. Example: **Switchover**, **Failover**, **Start**, or **Stop**.
- **Role:** Select **Primary** or **Standby** based on the system role. By default, the script is configured for both primary and standby roles for a given system.
- **Credential Type:** Select **Normal Host Credentials** or **Privileged Host Credentials** for users with root privileges.

Click **Save**.

8. Use the above steps to associate the pre-scripts and post-scripts for the standby site.

30.8.3.2 Associating Pre-Scripts and Post-Scripts Using EMCLI Commands

To associate a pre-script or post-script with Oracle Site Guard, run the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_script
    -system_name= "name"
    -operation="operation_name"
    -script_type="script_type"
    -host_name="name of the host"
    -path="path of the script"
    -all_hosts="true"
    -credential_type="type"
    -role="role"
```

Parameter	Description
-system_name	Specify the system on which you are performing the operation.
-operation	The function of the operation. Example: <i>Switchover</i> , <i>Failover</i> , <i>Start</i> , or <i>Stop</i> .
-script_type	The type of script, depending on the function you want to perform select one of the following options: <ul style="list-style-type: none"> ■ Pre-Script ■ Post-Script
-path	Enter the path to the script.
-host_name	The name of the host where the script will be run. Note: Ensure that the hostname is part of the system specified in <code>system_name</code> .
-all_hosts	Specify this optional flag to enable the script to run on all the hosts in the system. This parameter overrides the <code>host_name</code> .
-credential_type	Specify <code>HostNormal</code> credentials or <code>HostPrivileged</code> credentials for users with root privileges.
-role	Specify the role of the system when the script is run. For example: <code>Primary</code> or <code>Standby</code> .

30.8.4 Associating Storage Scripts

You can associate storage scripts (created in ["Creating Storage Scripts"](#)) for the Oracle Site Guard operation workflow.

You can associate the storage scripts using one of the following options:

- [Associating Storage Scripts Using Enterprise Manager Cloud Control Console](#)
- [Associating Storage Scripts Using EMCLI Commands](#)

30.8.4.1 Associating Storage Scripts Using Enterprise Manager Cloud Control Console

To associate storage scripts for the primary site, complete the following steps:

1. Log in to Enterprise Manager as an `EM_CLOUD_ADMINISTRATOR` user.
2. Select **Targets** and then select **Systems**.
The **Systems** page is displayed.
3. Select the primary system (created in ["Creating Generic Systems for the Primary and Standby Sites"](#)).
4. Click **Generic System > Site Guard > Configure**.
The **Site Guard Configuration** page is displayed.
5. Click the **Storage Scripts** tab.
6. Click **Add**.
The **Add Storage Scripts** page is displayed.
7. Enter the following details:
 - **Script Path:** Enter the path to the script or click the search icon, and specify the path to the script.
 - **Target Hosts:** Select the target name.
 - **Script Type:** The type of script, depending on the function you want to perform, select one of the following options:
 - Mount
 - UnMount
 - **Storage-Switchover**
 - **Storage-Failover**
 - **Operation Type:** The function of the operation. Example: **Switchover** or **Failover**.
 - **Credential Type:** Select **Normal Host Credentials** or **Privileged Host Credentials** for users with `root` privileges.

Click **Save**.
8. To associate the storage scripts for the standby site, follow steps 1-7.

30.8.4.2 Associating Storage Scripts Using EMCLI Commands

You must associate the following storage scripts:

- [Mount Scripts for Primary and Standby Sites](#)

- [Unmount Script for Primary and Standby Sites](#)
- [Switchover Script for Primary and Standby Sites](#)
- [Failover Script for Primary and Standby Sites](#)

Mount Scripts for Primary and Standby Sites

To associate a mount script, run the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_script
  -system_name="system_name"
  -operation="operation_name"
  -script_type="Mount"
  -host_name="name of the host"
  -path="path of the script"
  -all_hosts="true"
  -credential_type="type"
```

Unmount Script for Primary and Standby Sites

To associate a pre-script or post-script, run the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_script
  -system_name="system_name"
  -operation="operation_name"
  -script_type="UnMount"
  -host_name="name of the host"
  -path="path of the script"
  -all_hosts="true"
  -credential_type="type"
```

Switchover Script for Primary and Standby Sites

To associate a pre-script or post-script, run the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_script
  -system_name="system_name"
  -operation="operation_name"
  -script_type="Storage-Switchover"
  -host_name="name of the host"
  -path="path of the script"
  -all_hosts="true"
  -credential_type="type"
```

Failover Script for Primary and Standby Sites

To associate a pre-script or post-script, run the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_script
  -system_name="system_name"
  -operation="operation_name"
  -script_type="Storage-Failover"
  -host_name="name of the host"
  -path="path of the script"
  -all_hosts="true"
  -credential_type="type"
```

30.9 Executing Oracle Site Guard Operations

An operation plan contains the execution flow for the Oracle Site Guard operation. You can use it to define the order in which steps of an operation are executed. To execute any Oracle Site Guard operation, you must create an operation. It contains the execution flow for a Oracle Site Guard operation. For example, stopping Oracle HTTP Servers, stopping the Managed Servers and Administration Server in a WebLogic domain, and so on. You can either use the default operation plan or update it to change the order of targets within their corresponding steps.

You can save an operation plan to the repository, and execute it as needed.

Ensure that you must complete the following steps before you perform an operation:

- [Creating an Operation Plan](#)
- [Updating an Operation Plan](#)
- [Running Precheck Utility](#)
- [Submitting an Operation Plan](#)
- [Monitoring an Operation Plan](#)

30.9.1 Creating an Operation Plan

You can create an operation plan by running the following `emcli` commands in the command-line interface:

For switchover or failover operations:

```
emcli create_operation_plan
      -name="name"
      -primary_system_name="primary_system_name"
      -standby_system_name="standby_system_name"
      -operation_plan="operation_name"
```

For starting or stopping a site:

```
emcli create_operation_plan
      -name="name"
      -system_name="name"
      -operation_plan="operation_name"
```

Parameter	Description
<code>name</code>	Set the name of the operation plan.
<code>primary_system_name</code>	Set the name of the primary system. This parameter is set for switchover or failover operation only.
<code>standby_system_name</code>	Set the name of the standby system. This parameter is set for switchover or failover operation only.
<code>system_name</code>	Enter the name of the system.
<code>operation_plan</code>	Enter the name of the operation plan.

For a sample of the `emcli` command for creating an operation plan using the command-line interface, see [Example F-2](#) in [Appendix F.2, "create_operation_plan"](#).

30.9.2 Updating an Operation Plan

You can update an operation plan as follows:

- [Changing Execution Orders](#)
- [Updating Execution Modes](#)
- [Disabling a Step](#)
- [Updating Error Modes](#)

Changing Execution Orders

You can modify the order in which the steps are executed in an operation plan. For example, you can start the Oracle Identity Manager domain before starting any other Oracle WebLogic Server domain in a site or the order of an individual step in an operation plan, by running the following `emcli` command in the command-line interface:

```
emcli update_operation_plan
      -name="plan_name"
      -step_number="7"
      -move="Up"
```

Updating Execution Modes

The execution mode determines whether the steps pertaining to a target type in the site runs in parallel (executed simultaneously) or in serial mode. The execution mode can be either `Serial` or `Parallel`. You can update the execution mode by running the following `emcli` command in the command-line interface:

```
emcli update_operation_plan
      -name="plan_name"
      -step_number="2"
      -execution_mode="Parallel"
```

Disabling a Step

You can disable any step in the operation plan by running the following `emcli` command in the command-line interface:

```
emcli update_operation_plan
      -name="plan_name"
      -step_number="2"
      -enabled="false"
```

Updating Error Modes

For more information, see ["Updating Error Modes in an Operation Plan"](#).

30.9.3 Running Precheck Utility

Oracle Site Guard automatically runs the precheck utility before performing any operation. You can also run the precheck utility separately, before executing any Oracle Site Guard operations. Oracle Site Guard performs the following prechecks:

- Checks whether the Fusion Middleware Farms running on the primary is down before performing a failover operation.
- Checks the agent status on all hosts involved in the operation.
- Checks if any new targets are added to the generic system after the operation plan is created.

- Checks whether all targets involved in the operation plan exist in the Enterprise Manager repository.
- Detects if any targets are moved out or deleted from the generic system after the operation plan is created.
- Asserts the existence of all configured scripts (pre/post/mount/unmount/storage role reversal) on their respective target hosts.
- Runs Oracle Data Guard Broker prechecks to ascertain whether the Database is ready for role reversal (for switchover/failover operation)
- Performs Database Role Checks

You must run the following `emcli` command in the command-line interface:

```
emcli run_prechecks
      -operation_plan="operation_plan_name"
```

Parameter	Description
<code>-operation_plan</code>	Enter the name of your operation plan.

You can also monitor the status of a precheck operation using Enterprise Manager Cloud Control.

Note: For more information, see [Appendix F.17, "run_prechecks"](#).

30.9.4 Submitting an Operation Plan

You must submit an operation plan by running the following `emcli` command in the command-line interface:

```
emcli submit_operation_plan
      -name="operation plan_name"
      [-run_prechecks={true|false}]
```

Parameter	Description
<code>-name</code>	Enter the name of the operation plan.
<code>-run_prechecks</code>	Enter <code>false</code> , if you do not want to run precheck. For more information, see "Running Precheck Utility" .

Note: For more information, see [Appendix F.18, "submit_operation_plan"](#).

30.9.5 Monitoring an Operation Plan

To monitor an operation plan submitted for execution, complete the following steps:

1. Log in to Enterprise Manager Cloud Control Console as an `EM_CLOUD_ADMINISTRATOR` user.
2. Click **Enterprise > Provisioning and Patching > Procedure Activity**.
The **Provisioning** page is displayed.
3. Click the **Procedure Activity** tab.

Note: You can also verify the status by running the following `emcli` command in the command-line interface:

```
get_instance_status_instance="GUID"
```

To get the GUID information, run the following command:

```
emcli get_instances  
-type="SiteGuard"
```

30.10 Error Management Framework

Oracle Site Guard uses the Enterprise Manager Cloud Control deployment procedures framework to orchestrate disaster recovery operations on remote hosts. The framework provides error management support through error modes (stop and continue). In a disaster recovery scenario, it is very likely that things may go wrong. For example, some hosts might go down, become unreachable, or some servers might not start. To address such failures, Oracle Site Guard provides an option to define the error mode for individual steps and also lets you enable or disable steps. By default, the error mode is stop, and the run mode is enabled. This section includes the following topics:

- [Error Modes](#)
- [Updating Error Modes in an Operation Plan](#)
- [Retrying a Failed Operation](#)

Note: For more information, see "[Troubleshooting Oracle Site Guard Issues](#)".

30.10.1 Error Modes

You can define the following error modes for individual targets in a step for any given operation plan:

- [Stop Error Mode](#)
- [Continue Error Mode](#)

30.10.1.1 Stop Error Mode

The execution flow stops if the step fails. The status of the step becomes **Action Required**. You must manually confirm this failure from Enterprise Manager Cloud Control console to restart the execution. The execution flow continues after the confirmation, but the failed step is not retried. The failed step can be retried at the job level from the console but the status of the retry operation is not reflected at the target level status or at the top-level step status. This is the default error mode. See [Figure 30–3](#) and [Figure 30–4](#).

Figure 30–3 Status Details

Select	Name	Type	Status
<input type="checkbox"/>	▼ Run PreChecks	Procedure Step	✓
<input type="checkbox"/>	RunPreChecks	Computational	✓
<input type="checkbox"/>	Run_PreCheckScript_Parallel	Parallel	✓
<input type="checkbox"/>	Run_PreCheckScript_Serial	Rolling	⬇
<input type="checkbox"/>	Run_DatabasePreChecks_Parallel	Parallel	✓
<input type="checkbox"/>	Run_DatabasePreChecks_Serial	Rolling	⬇
<input type="checkbox"/>	▶ Run PreScripts	Procedure Step	✓
<input type="checkbox"/>	Start_Database_Parallel	Parallel	✓
<input type="checkbox"/>	Start_Database_Serial	Rolling	⬇
<input type="checkbox"/>	Confirm Start Database Execution Status	Manual	⬇
<input type="checkbox"/>	▼ Start_Domain_Parallel	Parallel	⚠
<input type="checkbox"/>	▼ /EMGC_EMGC_DOMAIN/EMGC_DOMAIN	host	⚠
<input type="checkbox"/>	▼ Start_NodeManager_Parallel_Domain_Parallel	Parallel	⚠
<input type="checkbox"/>	▼ host.example.com	host	⚠
<input type="checkbox"/>	StartNodeManager_Parallel_Domain_Parallel	Directive	✗
<input type="checkbox"/>	Start_NodeManager_Serial_Domain_Parallel	Rolling	Failed - Continue on Error
<input type="checkbox"/>	Confirm Start NodeManager Execution Status	Manual	⬇
<input type="checkbox"/>	▼ Start_AdminServer_Parallel_Domain_Parallel	Parallel	⚠
<input type="checkbox"/>	▼ host.example.com	host	⚠
<input type="checkbox"/>	StartAdminServer_Parallel_Domain_Parallel	Component	✗
<input type="checkbox"/>	Start_AdminServer_Serial_Domain_Parallel	Rolling	⬇
<input type="checkbox"/>	Confirm Start Weblogic AdminServer Execution Status	Manual	✓
<input type="checkbox"/>	▶ Start_ManagedServer_Parallel_Domain_Parallel	Parallel	⚠
<input type="checkbox"/>	Start_ManagedServer_Serial_Domain_Parallel	Rolling	⬇
<input type="checkbox"/>	Confirm Start Weblogic ManagedServer Execution Status	Manual	✓
<input type="checkbox"/>	Start_Domain_Serial	Rolling	⬇
<input type="checkbox"/>	Start_OracleInstance_Parallel	Parallel	✓
<input type="checkbox"/>	Start_OracleInstance_Serial	Rolling	⬇
<input type="checkbox"/>	Confirm Start Oracle Instance Execution Status	Manual	✓
<input type="checkbox"/>	▼ Run PostScripts	Procedure Step	✓
<input type="checkbox"/>	Run_Script_Parallel	Parallel	✓
<input type="checkbox"/>	Run_Script_Serial	Rolling	⬇
<input type="checkbox"/>	Confirm Run Script Execution Status	Manual	✓
<input type="checkbox"/>	Update SiteGuard Schema	Computational	✓

Figure 30–4 Stop Error Mode

▼ **Confirm Start NodeManager Execution Status** ✕

Type Manual Start Date Aug 7, 2012 1:41:16 AM PDT

Elapsed 1 days, 13 hours, 35 minutes, 31 Completed Date

Time seconds

Information

Please make sure all of the instructions are completed before you confirm.

Instructions

Note

30.10.1.2 Continue Error Mode

In this error mode, execution flow continues even if the step fails. The status of the step shows **Failed**, but the operation continues and the top-level step status shows **Completed with Errors**. Figure 30–5 shows an example of continue error mode.

Figure 30–5 Continue Error Mode

Select	Name	Type	Status
<input type="checkbox"/>	▷ Run PreChecks	Procedure Step	
<input type="checkbox"/>	▷ Run PreScripts	Procedure Step	
<input type="checkbox"/>	Start_Database_Parallel	Parallel	
<input type="checkbox"/>	Start_Database_Serial	Rolling	
<input type="checkbox"/>	Confirm Start Database Execution Status	Manual	
<input type="checkbox"/>	▽ Start_Domain_Parallel	Parallel	
<input type="checkbox"/>	▽ /EMGC_EMGC_DOMAIN/EMGC_DOMAIN	host	
<input type="checkbox"/>	▽ Start_NodeManager_Parallel_Domain_Parallel	Parallel	
<input type="checkbox"/>	▽ adc2120767.us.oracle.com	host	
<input type="checkbox"/>	StartNodeManager_Parallel_Domain_Parallel	Directive	
<input type="checkbox"/>	Start_NodeManager_Serial_Domain_Parallel	Rolling	
<input checked="" type="checkbox"/>	Confirm Start NodeManager Execution Status	Manual	
<input type="checkbox"/>	▷ Start_AdminServer_Parallel_Domain_Parallel	Parallel	
<input type="checkbox"/>	▽ Start_AdminServer_Serial_Domain_Parallel	Rolling	Action Required
<input type="checkbox"/>	StartAdminServer_Serial_Domain_Parallel	Component	
<input type="checkbox"/>	Confirm Start Weblogic AdminServer Execution Status	Manual	
<input type="checkbox"/>	▽ Start_ManagedServer_Parallel_Domain_Parallel	Parallel	
<input type="checkbox"/>	StartManagedServer_Parallel_Domain_Parallel	Component	
<input type="checkbox"/>	▽ Start_ManagedServer_Serial_Domain_Parallel	Rolling	
<input type="checkbox"/>	StartManagedServer_Serial_Domain_Parallel	Component	
<input type="checkbox"/>	Confirm Start Weblogic ManagedServer Execution Status	Manual	
<input type="checkbox"/>	▷ Start_Domain_Serial	Rolling	
<input type="checkbox"/>	▷ Start_OracleInstance_Parallel	Parallel	
<input type="checkbox"/>	▽ Start_OracleInstance_Serial	Rolling	
<input type="checkbox"/>	StartOracleInstance_Serial	Directive	
<input type="checkbox"/>	Confirm Start Oracle Instance Execution Status	Manual	
<input type="checkbox"/>	▷ Run PostScripts	Procedure Step	
<input type="checkbox"/>	Update SiteGuard Schema	Computational	

30.10.2 Updating Error Modes in an Operation Plan

You can update the error modes in an operation plan by running the following `emcli` command in the command-line interface:

```
emcli update_operation_plan
      -name="plan_name"
      -step_number={step number}
      -target_host={host name}
      -error_mode={error mode}
```

Parameter	Description
-name	The name of the operation plan.
-step_number	Number of the step which should be updated
-target_host	The name of the system. Enter this option for Start or Stop operation.
-error_mode	The error mode type. For example, Stop or Enabled.

Figure 30–6 shows an example of a user-defined operation plan.

Figure 30–6 Updating Error Mode

```
$ emcli get_operation_plan_details -name="switchover-to-STBYSOA1"
```

Step No	Operation	Target Name	Target Host	Error Mode	Run Mode
1	Run Script	/u01/app/oracle/admin/soa_instance/scripts/find-jar.sh something	SOAHOST1	Stop	Enabled
2	Run Script	/u01/app/oracle/admin/soa_instance/scripts/find-jar.sh something	SOAHOST2	Stop	Enabled
3	Stop OracleInstance	/u02/oracle/product/Middleware/Oracle_WT1/instances/instance1	SOAHOST1	Stop	Enabled
4	Stop OracleInstance	/u02/oracle/product/Middleware/Oracle_WT2/instances/instance2	SOAHOST2	Stop	Enabled
5	Stop ManagedServer	/base_domain/base_domain/bam_server1	SOAHOST1	Stop	Enabled
6	Stop ManagedServer	/base_domain/base_domain/bam_server2	SOAHOST2	Stop	Enabled
7	Stop ManagedServer	/base_domain/base_domain/soa_server1	SOAHOST1	Stop	Enabled
8	Stop ManagedServer	/base_domain/base_domain/soa_server2	SOAHOST2	Stop	Enabled
9	Stop NodeManager	/u02/oracle/product/Middleware/wlserver_10.3	SOAHOST1	Stop	Enabled
10	Stop NodeManager	/u02/oracle/product/Middleware/wlserver_10.3	SOAHOST2	Stop	Enabled
11	Stop AdminServer	/base_domain/base_domain/AdminServer	SOAHOST1	Stop	Enabled
12	Run Script	/u01/app/oracle/admin/soa_instance/scripts/umount.sh	SOAHOST1	Stop	Disabled
13	Run Script	/u01/app/oracle/admin/soa_instance/scripts/umount.sh	SOAHOST2	Stop	Disabled
14	Run Script	/u01/app/oracle/admin/soa_instance/scripts/find-jar.sh something	SOAHOST1	Stop	Enabled
15	Run Script	/u01/app/oracle/admin/soa_instance/scripts/find-jar.sh something	SOAHOST2	Stop	Enabled
16	Run Script	/u01/app/oracle/admin/soa_instance/scripts/find-jar.sh something	STBYSOA1	Stop	Enabled
17	Run Script	/u01/app/oracle/admin/soa_instance/scripts/find-jar.sh something	STBYSOA2	Stop	Enabled
18	Run Script	/u01/app/oracle/admin/soa_instance/scripts/mount.sh	STBYSOA1	Stop	Disabled
19	Run Script	/u01/app/oracle/admin/soa_instance/scripts/mount.sh	STBYSOA2	Stop	Disabled
20	Switchover Database	Database-STBYSOA1	STBYSOA1	Stop	Enabled
21	Start NodeManager	/u02/oracle/product/Middleware/wlserver_10.3	STBYSOA1	Stop	Enabled
22	Start NodeManager	/u02/oracle/product/Middleware/wlserver_10.3	STBYSOA2	Stop	Enabled
23	Start AdminServer	/domain/base_domain/AdminServer	STBYSOA1	Stop	Enabled
24	Start ManagedServer	/domain/base_domain/bam_server1	STBYSOA1	Stop	Enabled
25	Start ManagedServer	/domain/base_domain/bam_server2	STBYSOA2	Stop	Enabled
26	Start ManagedServer	/domain/base_domain/soa_server1	STBYSOA1	Stop	Enabled
27	Start ManagedServer	/domain/base_domain/soa_server2	STBYSOA2	Stop	Enabled
28	Start OracleInstance	/u02/oracle/product/Middleware/Oracle_WT1/instances/instance1	STBYSOA1	Continue	Enabled
29	Start OracleInstance	/u02/oracle/product/Middleware/Oracle_WT2/instances/instance2	STBYSOA2	Continue	Enabled
30	Run Script	/u01/app/oracle/admin/soa_instance/scripts/find-jar.sh something	STBYSOA1	Stop	Enabled
31	Run Script	/u01/app/oracle/admin/soa_instance/scripts/find-jar.sh something	STBYSOA2	Stop	Enabled

30.10.3 Retrying a Failed Operation

To retry a failed operation, complete the following steps:

1. Log in to Enterprise Manager Cloud Control Console as an EM_CLOUD_ADMINISTRATOR user.
2. Click **Enterprise > Provisioning and Patching > Procedure Activity**.
The **Provisioning** page is displayed.
3. Click the **Procedure Activity** tab.
4. Select the failed operation, and click **Action Required**.
5. In **Embedded Procedure Step**, click **Action Required**.
6. Select the failed operation, and click **Failed**.
7. In **Target**, select the failed operation, and click **Failed**.
8. Switch to **Classic View**.
9. Click **Enterprise > Provisioning and Patching > Procedure Activity Credentials**.
10. Click **Procedure Activity**.
11. Select the failed operation, and click **Action Required**.
12. In **Embedded Procedure Step**, click **Action Required**.
13. Select the failed operation, and click **Action Required**.
14. Click **Confirm**.

30.11 Managing a Site Using Oracle Site Guard

You can use emcli commands to execute the following Oracle Site Guard operations:

- [Stopping a Site](#)
- [Starting a Site](#)

- [Performing Site Switchover](#)
- [Performing Site Failover](#)

Note: See [Appendix F, "Oracle Site Guard Command-Line Interface Reference"](#) for the list of `emcli` commands to manage an Oracle Site Guard configuration directly from the command-line interface.

30.11.1 Stopping a Site

To stop a site, run the following `emcli` command in the command-line interface:

```
emcli submit_operation_plan
      -name="stop-site1"
      -run_prechecks="true"
```

Parameter	Description
-name	Specify the name of the site that you want to stop.
-run_prechecks	Enter true or false. The value of this parameter is true, by default.

30.11.2 Starting a Site

To start a site, run the following `emcli` command in the command-line interface:

```
emcli submit_operation_plan
      -name="start-site1"
      -run_prechecks="true"
```

Parameter	Description
-name	Specify the name of the site that you want to start.
-run_prechecks	Enter true or false. The value of this parameter is true, by default.

30.11.3 Performing Site Switchover

To perform a site switchover, run the following `emcli` command in the command-line interface:

```
emcli submit_operation_plan
      -name="switchover-site1"
      -run_prechecks="true"
```

Parameter	Description
-name	Specify the name of the site for which you want to perform a switchover.
-run_prechecks	Enter true or false.

30.11.4 Performing Site Failover

To perform a site failover, run the following `emcli` command in the command-line interface:

```
emcli submit_operation_plan
      -name="failover-site1"
```

```
-run_prechecks="true"
```

Parameter	Description
-name	Specify the name of the site for which you want to perform a failover.
-run_prechecks	Enter true or false.

After performing a failover operation, you must manually reinstate the database manually. For more information, see "How to Reinststate a Database" in the *Oracle Data Guard Broker*.

Example Scenario: Using Oracle Site Guard

This chapter uses the Oracle Business Intelligence Enterprise Edition (EE) enterprise deployment topology as an example to illustrate the steps required to use Oracle Site Guard to manage disaster recovery on the production site and standby site. To use Oracle Site Guard, complete the following tasks:

- [Task 1: Setting Up Oracle Business Intelligence Enterprise Deployment](#)
- [Task 2: Discovering Targets for the Primary Site and the Standby Site](#)
- [Task 3: Creating Production and Standby Systems for Oracle Business Intelligence](#)
- [Task 4: Creating Credentials](#)
- [Task 5: Configuring the Software Library](#)
- [Task 6: Creating Oracle Site Guard Configuration](#)
- [Task 7: Associating Credentials for Site](#)
- [Task 8: Creating Pre-Scripts and Post-Scripts](#)
- [Task 9: Associating Storage Scripts](#)
- [Task 10: Creating Operation Plans](#)
- [Task 11: Starting BISystem1](#)
- [Task 12: Stopping BISystem1](#)
- [Task 13: Running the Oracle Site Guard Pre-Check Utility](#)
- [Task 14: Performing Site Switchover](#)
- [Task 15: Performing Site Failover](#)

31.1 Task 1: Setting Up Oracle Business Intelligence Enterprise Deployment

Set up your Oracle Business Intelligence enterprise deployment, as described in the *Oracle Fusion Middleware Enterprise Deployment Guide for Oracle Business Intelligence* guide.

Ensure that the following requirements are met:

- Ensure that host names are configured, as described in the section "Host Names for the Oracle Business Intelligence Production Site and Standby Site Hosts" in *Oracle Fusion Middleware Disaster Recovery Guide*.
- Ensure that virtual IP addresses and virtual host names are configured, as described in the section "Virtual IP Addresses and Virtual Host Names for the

Oracle Business Intelligence Production Site and Standby Site Hosts" in *Oracle Fusion Middleware Disaster Recovery Guide*.

- Read the section "Directory Structure Recommendations for Oracle Business Intelligence" in *Oracle Fusion Middleware Disaster Recovery Guide*.
- Ensure that the Oracle Business Intelligence production site is configured, as described in the section "Creating the Production Site for the Oracle Business Intelligence Topology" in *Oracle Fusion Middleware Disaster Recovery Guide*.
- Ensure that the Oracle Business Intelligence standby site is configured, as described in the section "Creating the Standby Site" in *Oracle Fusion Middleware Disaster Recovery Guide*.

31.2 Task 2: Discovering Targets for the Primary Site and the Standby Site

Discover the targets for the Oracle BI Enterprise Edition Primary Site and the Standby Site on the Enterprise Manager Cloud Control 12c Release 1 (12.1.0.2). For more information, see "[Discovering Targets on the Primary Site and the Standby Site](#)".

The following targets are available:

- Administration Server
- Managed Servers (bi_server1 and bi_server2)
- OPMN managed system components (WEBHOST1 and WEBHOST2)
- Oracle RAC Database instances (CUSTDBHOST1 and CUSTDBHOST2)

Note: Oracle Business Intelligence OPMN managed system components are not discovered in Enterprise Manager Cloud Control. To manage Oracle Business Intelligence OPMN managed system components, create custom scripts, as described in "[Creating Pre-Scripts and Post-Scripts for Start or Stop Operations](#)".

[Figure 31–1](#) and [Figure 31–2](#) show the available Oracle Fusion Middleware Farm and RAC Database target.

Figure 31–1 Oracle Fusion Middleware Targets

Name	Type	Status	Member Status	Compliance Score (%)	Target Version
BISystem1Farm01_bifoundation_domain	Oracle Fusion Middleware Farm	n/a	4 0 0 2	n/a	10.3.5.0
bifoundation_domain	Oracle WebLogic Domain	n/a	4 0 0 0	n/a	10.3.5.0
AdminServer	Oracle WebLogic Server	0	0 0 0 0	n/a	10.3.5.0
bi_cluster	Oracle WebLogic Cluster	2	0 0 0 0	n/a	10.3.5.0
bi_server1	Oracle WebLogic Server	0	0 0 0 0	n/a	10.3.5.0
bi_server2	Oracle WebLogic Server	0	0 0 0 0	n/a	10.3.5.0
mds-ovsm	Metadata Repository	n/a	0 0 0 0	n/a	n/a
ohs1	Oracle HTTP Server	0	0 0 0 0	n/a	11.1.1.4.0
ohs2	Oracle HTTP Server	0	0 0 0 0	n/a	11.1.1.4.0
BISystem2Farm01_bifoundation_domain	Oracle Fusion Middleware Farm	n/a	0 6 0 0	n/a	10.3.5.0

Figure 31–2 Database Targets

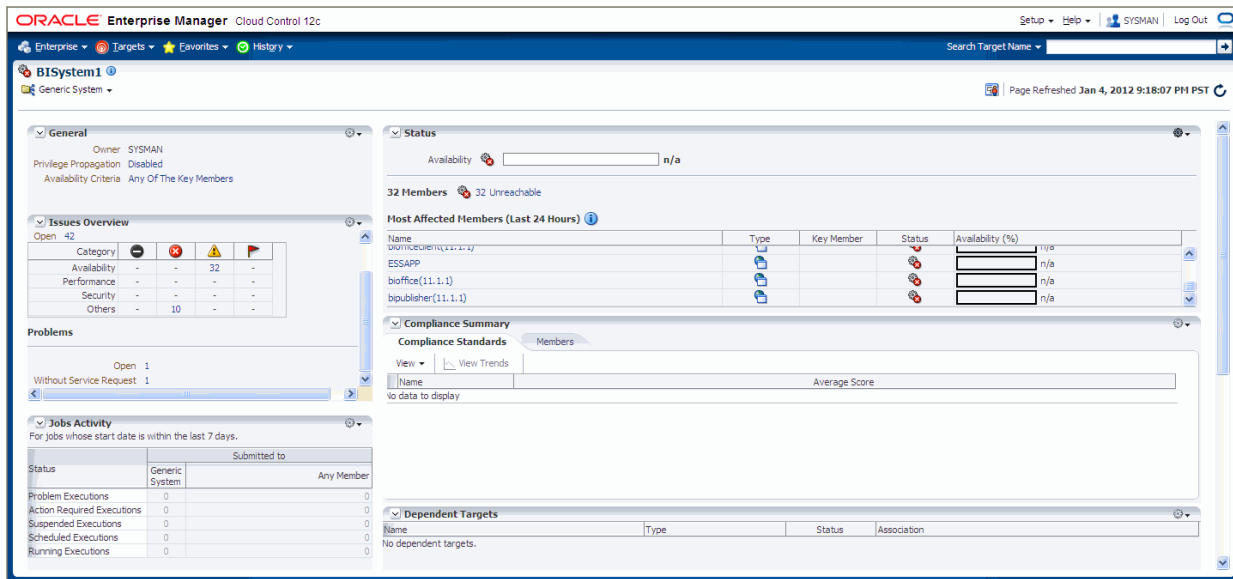
Select	Name	Type	Status	Incidents	Compliance Violations	Average Compliance score	Version	Sessions: CPU	Sessions: I/O	Sessions: Other	Instance CPU (%)
<input type="radio"/>	CUSTDBHOST1	Cluster Database: Primary	0	1 0 0	0 0 0	-	11.2.0.2.0	0	0	0	0
<input type="radio"/>	CUSTDBHOST2	Cluster Database: Primary	0	2 0 0	0 0 0	-	11.2.0.2.0	0	0	0	0

31.3 Task 3: Creating Production and Standby Systems for Oracle Business Intelligence

Complete the steps listed in "Creating Generic Systems for the Primary and Standby Sites". Enter BISystem1 and BISystem2 as the name for the production and standby systems respectively.

Figure 31–3 shows the BISystem1 system.

Figure 31–3 Generic System for the Production and Standby Site



31.4 Task 4: Creating Credentials

For more information, see ["Creating Credentials"](#).

31.5 Task 5: Configuring the Software Library

For more information, see ["Configuring the Software Library"](#)

31.6 Task 6: Creating Oracle Site Guard Configuration

Add the configuration for the BISystem1 and BISystem2 using one of the following options:

- [Associating Oracle Business Intelligence Sites Using Enterprise Manager Cloud Control Console](#)
- [Associating Oracle Business Intelligence Sites Using EMCLI Commands](#)

31.6.1 Associating Oracle Business Intelligence Sites Using Enterprise Manager Cloud Control Console

To associate BISystem2 with BISystem1, complete the following steps:

1. Log in to Enterprise Manager as an EM_CLOUD_ADMINISTRATOR user.
2. Select **Targets**, and from the drop-down menu, select **Systems**.
The **Systems** page is displayed.
3. Select **BISystem1**.
4. Click **Generic System > Site Guard > Configure**.
The **Site Guard Configuration** page is displayed.
5. In the **Standby System(s)** section, click **Add**.
The **Search and Select: Standby Systems** page is displayed.

6. Choose **BISystem2**, and click **Select**.
7. Click **Save**.
The **Site Guard configuration saved successfully** dialog box is displayed.
8. Click **OK**.
9. Perform steps 1-8 to associate **BISystem1** for **BISystem2**.

31.6.2 Associating Oracle Business Intelligence Sites Using EMCLI Commands

To add the configuration for the primary and standby sites, run the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_configuration
      -primary_system_name="BISystem1"
      -standby_system_name="BISystem2"
```

See [Appendix F.3, "create_siteguard_configuration"](#) for more information.

To display information about the association between existing primary sites and standby sites, run the following `emcli` commands in the command-line interface:

```
emcli get_siteguard_configuration
      -primary_system_name="BISystem1"
      -standby_system_name="BISystem2"
```

31.7 Task 7: Associating Credentials for Site

Associate the credentials for the **BISystem1** and **BISystem2** using one of the following options:

- [Associating Credentials for Oracle Business Intelligence Sites Using Enterprise Manager Cloud Control Console](#)
- [Associating Credentials for Oracle Business Intelligence Sites Using EMCLI Commands](#)

31.7.1 Associating Credentials for Oracle Business Intelligence Sites Using Enterprise Manager Cloud Control Console

To associate the credentials for **BISystem1**, complete the following steps:

1. Log in to Enterprise Manager as an `EM_CLOUD_ADMINISTRATOR` user.
2. Select **Targets** and then select **Systems**.
The **Systems** page is displayed.
3. Select **BISystem1**.
4. Click **Generic System > Site Guard > Configure**.
The **Site Guard Configuration** page is displayed.
5. Click **Credentials**.
6. In the **Normal Host Credentials** section, click **Add**.
The **Add Normal Host Credentials** page is displayed.
7. Enter the following details:

Element	Description
Target	Select the target name.
Use Preferred Credentials	If you are using preferred credentials, then select the checkbox.
Named Credential	If you are using named credentials, then select the credential name.

Click **Save**.

8. In the **Privileged Host Credentials** section, click **Add**.

The **Add Privileged Host Credentials** page is displayed.

9. Enter the following details:

Element	Description
Target	Select the target name.
Use Preferred Credentials	If you are using preferred credentials, then select the checkbox.
Named Credential	If you are using named credentials, then select the credential name.

Click **Save**.

10. In the **Oracle WebLogic Administration Credentials** section, click **Add**.

The **Add Oracle WebLogic Administration Credentials** page is displayed.

11. Enter the following details:

Element	Description
Target	Select the target name.
Use Preferred Credentials	If you are using preferred credentials, then select the checkbox.
Named Credential	If you are using named credentials, then select the credential name.

Click **Save**.

12. In the **Database Credentials** section, click **Add**.

The **Add Database Credentials** page is displayed.

13. Enter the following details:

Element	Description
Target	Select the target name
Use Preferred Credentials	If you are using preferred credentials, then select the checkbox.
Named Credential	If you are using named credentials, then select the credential name.

Click **Save**.

14. Choose the standby system, and click **Select**.
15. Use the above steps to associate the credentials for BISystem2.

31.7.2 Associating Credentials for Oracle Business Intelligence Sites Using EMCLI Commands

You must associate the named credentials for the following targets:

- Host (for normal user and users with `root` privileges)
- Host (users with `root` privileges)
- Oracle WebLogic Server
- Oracle Database

Create the named credentials by running the credential framework `emcli` commands for the following:

- [Creating Credentials for Host Targets](#)
- [Creating Credentials for Oracle WebLogic Server Targets](#)
- [Creating Credentials for Oracle Database Targets](#)

Creating Credentials for Host Targets

Specify credentials for the host on which Oracle Business Intelligence Enterprise Edition (EE) is installed and configured. Run the following `emcli` commands in the command-line interface:

BISystem1 for Host (Normal User)

```
emcli create_siteguard_credential_association
  -system_name="BISystem1"
  -credential_type="HostNormal"
  -credential_name="NC_HOSTNORMAL"
  -credential_owner="sysman"
```

BISystem1 for Host (Users with Root Privileges)

```
emcli create_siteguard_credential_association
  -system_name="BISystem1"
  -credential_type="HostPrivileged"
  -credential_name="NC_HOSTSUDO"
  -credential_owner="sysman"
```

BISystem2 for Host (Normal User)

```
emcli create_siteguard_credential_association
  -system_name="BISystem2"
  -credential_type="HostNormal"
  -credential_name="NC_HOSTNORMAL"
  -credential_owner="sysman"
```

BISystem2 for Host (Users with root Privileges)

```
emcli create_siteguard_credential_association
  -system_name="BISystem2"
  -credential_type="HostPrivileged"
  -credential_name="NC_HOSTSUDO"
  -credential_owner="sysman"
```

See [Appendix F.4, "create_siteguard_credential_association"](#) for more information.

Creating Credentials for Oracle WebLogic Server Targets

Specify the credentials for Oracle WebLogic Server by running the following `emcli` commands in the command-line interface:

BISystem1

```
emcli create_siteguard_credential_association
      -system_name="BISystem1"
      -credential_type="WLSAdmin"
      -credential_name="NC_WLSADMIN"
      -credential_owner="sysman"
```

BISystem2

```
emcli create_siteguard_credential_association
      -system_name="BISystem2"
      -credential_type="WLSAdmin"
      -credential_name="NC_WLSADMIN"
      -credential_owner="sysman"
```

See [Appendix F.4, "create_siteguard_credential_association"](#) for more information.

Creating Credentials for Oracle Database Targets

Specify credentials for Oracle Database by running the following `emcli` commands in the command-line interface:

BISystem1

```
emcli create_siteguard_credential_association
      -system_name="BISystem1"
      -credential_type="DatabaseSysdba"
      -credential_name="NC_BIDBINSTANCES"
      -credential_owner="sysman"
```

BISystem2

```
emcli create_siteguard_credential_association
      -system_name="BISystem2"
      -credential_type="DatabaseSysdba"
      -credential_name="NC_BIDBINSTANCES"
      -credential_owner="sysman"
```

See [Appendix F.4, "create_siteguard_credential_association"](#) for more information.

Validate that the credentials that are associated with the system, by running the following `emcli` commands in the command-line interface:

```
emcli get_siteguard_credential_association
      -system_name="system_name"
```

[Figure 31–4](#) shows the credentials associated with `BISystem1`.

Figure 31–4 Credentials Associated with BISystem1

```
[ BIHOST1 bin]$ ./emcli get_siteguard_credential_association -system_name="BISystem1"
```

Target Name	Credential Name	Credential
BIHOST1	NC_HOSTNORMAL	HostNormal
BIHOST1	NC_HOSTNORMAL	HostNormal
BIHOST1	NC_HOSTNORMAL	HostNormal
BIHOST1	NC_HOSTNORMAL	HostNormal
WEBHOST1	NC_HOSTNORMAL	HostNormal
WEBHOST2	NC_HOSTNORMAL	HostNormal
BIHOST2	NC_HOSTSUDO	HostPrivile
BIHOST2	NC_HOSTSUDO	HostPrivile
BIHOST2	NC_HOSTSUDO	HostPrivile
BIHOST2	NC_HOSTSUDO	HostPrivile
WEBHOST1	NC_HOSTSUDO	HostPrivile
WEBHOST2	NC_HOSTSUDO	HostPrivile
/BISystem1Farm01_bifoundation_domain/bifoundation_	NC_WLSADMIN	WLSAdmin
domain/AdminServer		
CUSTDBHOST1	NC_BIDBINSTANCES	DatabaseSys
CUSTDBHOST2	NC_BIDBINSTANCES	DatabaseSys

31.8 Task 8: Creating Pre-Scripts and Post-Scripts

Oracle Site Guard provides options to include user- specified scripts in the disaster recovery operation workflow. Create the following pre-scripts and post-scripts:

- [Creating Pre-Scripts and Post-Scripts for Start or Stop Operations](#)
- [Creating Pre-Scripts and Post-Scripts for Switchover or Failover Operations](#)

Note: After you create the required script, save them to the destination directory on each of the hosts from where the script is executed.

For example, /u01/ape/oracle/admin/bi_instance/sgscripts

For more information, see "[Associating Pre-Scripts and Post-Scripts](#)".

31.8.1 Creating Pre-Scripts and Post-Scripts for Start or Stop Operations

You can create Start and Stop scripts for the Oracle Business Intelligence OPMN managed system components. To manage these system components, create the following Start and Stop scripts:

- [Post-Script for Start Operation on BISystem1](#)
- [Pre-Script for Stop Operation on BISystem1](#)
- [Post-Script for Start Operation on BISystem2](#)
- [Pre-Script for Stop Operation on BISystem2](#)

Post-Script for Start Operation on BISystem1

Create a post-script for the start operation by running the following emcli commands in the command-line interface:

```
emcli create_siteguard_script
  -system_name= "BISystem1"
  -operation="Start"
  -script_type="Post-Script"
  -path="/u01/app/oracle/admin/bi_
```

```
instance/sgscripts/startbisystemcomponents.sh"
    -host_name="BIHOST1"
    -host_name="BIHOST2"
    -role="Primary"
    -credential_type="HostNormal"
```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

You can associate a post-script for the start operation by using Enterprise Manager Cloud Control Console, as described in "[Associating Pre-Scripts and Post-Scripts](#)".

Enter the following details in the **Add Pre/Post Scripts** page:

Element	Description
Script Path	Enter the following path of the script: /u01/app/oracle/admin/bi_ instance/sgscripts/startbisystemcomponents.sh
Target Host	Select BIHOST1 and BIHOST2.
Script Type	Enter Post-Script.
Operation Type	Enter Start.
Role	Enter Primary.
Credential Type	Enter Normal Host Credentials.

Pre-Script for Stop Operation on BISystem1

Create a pre- script for the stop operation by running the following emcli commands in the command-line interface:

```
emcli create_siteguard_script
    -system_name= "BISystem1"
    -operation="Stop"
    -script_type="Pre-Script"
    -path="/u01/app/oracle/admin/bi_
instance/sgscripts/stopbisystemcomponents.sh"
    -host_name="BIHOST1"
    -host_name="BIHOST2"
    -role="Primary"
    -credential_type="HostNormal"
```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

You can associate a post-script for the stop operation by using Enterprise Manager Cloud Control Console, as described in "[Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console](#)".

Enter the following details in the **Add Pre/Post Scripts** page:

Element	Description
Script Path	Enter the following path of the script: /u01/app/oracle/admin/bi_ instance/sgscripts/stopbisystemcomponents.sh
Target Host	Select BIHOST1 and BIHOST2.
Script Type	Enter Pre-Script.
Operation Type	Enter Stop.

Element	Description
Role	Enter Primary.
Credential Type	Enter Normal Host Credentials.

Post-Script for Start Operation on BISystem2

Create a post-script for the start operation by running the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_script
  -system_name= "BISystem2"
  -operation="Start"
  -script_type="Post-Script"
  -path="/u01/app/oracle/admin/bi_
instance/sgscripts/startbisystemcomponents.sh"
  -host_name="STBYBI1"
  -host_name="STBYBI2"
  -role="Primary"
  -credential_type="HostNormal"
```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

You can associate a pre-script for the stop operation by using Enterprise Manager Cloud Control Console, as described in "[Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console](#)".

Enter the following details in the **Add Pre/Post Scripts** page:

Element	Description
Script Path	Enter the following path of the script: <code>/u01/app/oracle/admin/bi_</code> <code>instance/sgscripts/startbisystemcomponents.sh</code>
Target Host	Select STBYBI1 and STBYBI2.
Script Type	Enter Pre-Script.
Operation Type	Enter Start.
Role	Enter Primary.
Credential Type	Enter Normal Host Credentials.

Pre-Script for Stop Operation on BISystem2

Create a post-script for the stop operation by running the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_script
  -system_name= "BISystem2"
  -operation="Stop"
  -script_type="Pre-Script"
  -path="/u01/app/oracle/admin/bi_
instance/sgscripts/stopbisystemcomponents.sh"
  -host_name="STBYBI1"
  -host_name="STBYBI2"
  -role="Primary"
  -credential_type="HostNormal"
```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

You can associate a pre-script for the stop operation by using Enterprise Manager Cloud Control Console, as described in ["Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console"](#).

Enter the following details in the **Add Pre/Post Scripts** page:

Element	Description
Script Path	Enter the following script path: /u01/app/oracle/admin/bi_ instance/sgscripts/stopbisystemcomponents.sh
Target Host	Select STBYBI1 and STBYBI2
Script Type	Enter Pre-Script
Operation Type	Enter Stop
Role	Enter Primary
Credential Type	Enter Normal Host Credentials

31.8.2 Creating Pre-Scripts and Post-Scripts for Switchover or Failover Operations

You can create the following pre-scripts and post-scripts for switchover and failover operations:

- [Pre-Script for Switchover Operation on BISystem1](#)
- [Post-Script for Switchover Operation on BISystem1](#)
- [Post-Script for Failover Operation on BISystem1](#)
- [Pre-Script for Switchover Operation on BISystem2](#)
- [Post-Script for Switchover Operation on BISystem2](#)
- [Post-Script for Failover Operation on BISystem2](#)

Pre-Script for Switchover Operation on BISystem1

Create a pre-script for the switchover operation by running the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_script
      -system_name= "BISystem1"
      -operation="Switchover"
      -script_type="Pre-Script"
      -path="/u01/app/oracle/admin/bi_
instance/sgscripts/stopbisystemcomponents.sh"
      -host_name="BIHOST1"
      -host_name="BIHOST2"
      -role="Primary"
      -credential_type="HostNormal"
```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

You can associate a pre-script for the stop operation by using Enterprise Manager Cloud Control Console, as described in ["Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console"](#).

Enter the following details in the **Add Pre/Post Scripts** page:

Element	Description
Script Path	Enter the following script path: /u01/app/oracle/admin/bi_ instance/sgscripts/stopbisystemcomponents.sh
Target Host	Select BIHOST1 and BIHOST2.
Script Type	Enter Pre-Script
Operation Type	Enter Switchover
Role	Enter Primary
Credential Type	Enter Normal Host Credentials

Post-Script for Switchover Operation on BISystem1

Create a post-script for the switchover operation by running the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_script
  -system_name= "BISystem1"
  -operation="Switchover"
  -script_type="Post-Script"
  -path="/u01/app/oracle/admin/bi_
instance/sgscripts/startbisystemcomponents.sh"
  -host_name="BIHOST1"
  -host_name="BIHOST2"
  -role="Standby"
  -credential_type="HostNormal"
```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

You can associate a pre-script for the stop operation by using Enterprise Manager Cloud Control Console, as described in "[Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console](#)".

Enter the following details in the **Add Pre/Post Scripts** page:

Element	Description
Script Path	Enter the following script path: /u01/app/oracle/admin/bi_ instance/sgscripts/startbisystemcomponents.sh
Target Host	Select BIHOST1 and BIHOST2.
Script Type	Enter Post-Script
Operation Type	Enter Switchover
Role	Enter Standby
Credential Type	Enter Normal Host Credentials

Post-Script for Failover Operation on BISystem1

Create a post-script for the failover operation by running the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_script
  -system_name= "BISystem1"
  -operation="failover"
  -script_type="Post-Script"
```

```

-path="/u01/app/oracle/admin/bi_
instance/sgscripts/startbisystemcomponents.sh"
-host_name="BIHOST1"
-host_name="BIHOST2"
-role="Standby"
-credential_type="HostNormal"

```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

You can associate a pre-script for the stop operation by using Enterprise Manager Cloud Control Console, as described in ["Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console"](#).

Enter the following details in the **Add Pre/Post Scripts** page:

Element	Description
Script Path	Enter the following script path: /u01/app/oracle/admin/bi_ instance/sgscripts/startbisystemcomponent s.sh
Target Host	Select BIHOST1 and BIHOST2.
Script Type	Enter Post-Script
Operation Type	Enter Failover
Role	Enter Standby
Credential Type	Enter Normal Host Credentials

Pre-Script for Switchover Operation on BISystem2

Create a pre-script for the switchover operation by running the following `emcli` commands in the command-line interface:

```

emcli create_siteguard_script
-system_name= "BISystem2"
-operation="Switchover"
-script_type="Pre-Script"
-path="/u01/app/oracle/admin/bi_
instance/sgscripts/stopbisystemcomponents.sh"
-host_name="STBYBI1"
-host_name="STBYBI2"
-role="Primary"
-credential_type="HostNormal"

```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

You can associate a pre-script for the stop operation by using Enterprise Manager Cloud Control Console, as described in [Section 30.8.3.1, "Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console"](#).

Enter the following details in the **Add Pre/Post Scripts** page:

Element	Description
Script Path	Enter the following script path: /u01/app/oracle/admin/bi_ instance/sgscripts/stopbisystemcomponents. sh

Element	Description
Target Host	Select STBYBI1 and STBYBI2
Script Type	Enter Pre-Script as the script type.
Operation Type	Specify Switchover as the operation type.
Role	Specify Primary
Credential Type	Enter Normal Host Credentials

Post-Script for Switchover Operation on BISystem2

Create a post-script for the switchover operation by running the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_script
      -system_name= "BISystem2"
      -operation="Switchover"
      -script_type="Post-Script"
      -path="/u01/app/oracle/admin/bi_
instance/sgscripts/startbisystemcomponents.sh"
      -host_name="STBYBI1"
      -host_name="STBYBI2"
      -role="Standby"
      -credential_type="HostNormal"
```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

You can associate a pre-script for the stop operation by using Enterprise Manager Cloud Control Console, as described in ["Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console"](#).

Enter the following details in the **Add Pre/Post Scripts** page:

Element	Description
Script Path	Enter the following script path: <code>/u01/app/oracle/admin/bi_ instance/sgscripts/startbisystemcomponents.s h</code>
Target Host	Select STBYBI1 and STBYBI2
Script Type	Enter Post-Script as the script type.
Operation Type	Specify Switchover as the operation type.
Role	Specify Primary.
Credential Type	Specify Normal Host Credentials as the credential type.

Post-Script for Failover Operation on BISystem2

Create a post-script for the failover operation, by running the following `emcli` commands in the command-line interface:

```
emcli create_siteguard_script
      -system_name= "BISystem2"
      -operation="failover"
      -script_type="Post-Script"
      -path="/u01/app/oracle/admin/bi_
instance/sgscripts/startbisystemcomponents.sh"
```

```
-host_name="STBYBI1"
-host_name="STBYBI2"
-role="Standby"
-credential_type="HostNormal"
```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

Associate a pre-script for the stop operation by using Enterprise Manager Cloud Control Console, as described in "[Associating Pre-Scripts and Post-Scripts Using Enterprise Manager Cloud Control Console](#)".

Enter the following details in the **Add Pre/Post Scripts** page:

Element	Description
Script Path	Enter the following script path: /u01/app/oracle/admin/bi_ instance/sgscripts/startbisystemcomponents.s h
Target Host	Select STBYBI1 and STBYBI2
Script Type	Enter Post-Script as the script type.
Operation Type	Specify Failover as the operation type.
Role	Specify Standby.
Credential Type	Specify Normal Host Credentials as the credential type.

31.9 Task 9: Associating Storage Scripts

You can associate the storage scripts for BISystem1 and BISystem2 using one of the following options:

- [Associating Storage Scripts for Oracle Business Intelligence Sites Using Enterprise Manager Cloud Control Console](#)
- [Associating Storage Scripts for Oracle Business Intelligence Sites Using EMCLI Commands](#)

31.9.1 Associating Storage Scripts for Oracle Business Intelligence Sites Using Enterprise Manager Cloud Control Console

To associate the storage scripts for BISystem1, complete the following steps:

1. Log in to Enterprise Manager as an EM_CLOUD_ADMINISTRATOR user.
2. Select **Targets** and then select **Systems**.
The **Systems** page is displayed.
3. Select **BISystem1**.
4. Click **Generic System > Site Guard > Configure**.
The **Site Guard Configuration** page is displayed.
5. Click the **Storage Scripts** tab.
6. Click **Add**.
The **Add Storage Scripts** page is displayed.

7. Enter the following details:

Element	Description
Script Path	Enter the following script path: <code>/u01/app/oracle/admin/bi_ instance/sgstoragescripts/switchvertobisystem1.sh</code>
Target Host	Select BIHOST1.
Script Type	Enter Storage-Switchover as the script type.
Operation Type	Specify Switchover as the operation type.
Credential Type	Specify Privileged Host Credentials as the credential type.

Click **Save**.

8. Use the above steps to associate the storage failover script for BISystem1. Ensure that you enter the following details:

Element	Description
Script Path	Enter the following script path: <code>/u01/app/oracle/admin/bi_ instance/sgstoragescripts/failovertobisystem1.sh</code>
Target Host	Select BIHOST1.
Script Type	Enter Storage-Switchover as the script type.
Operation Type	Specify Failover as the operation type.
Credential Type	Specify Privileged Host Credentials as the credential type.

Create the storage switchover and failover Script for BISystem2, as described in ["Associating Storage Scripts for Oracle Business Intelligence Sites Using Enterprise Manager Cloud Control Console"](#). Ensure that you enter the following details:

Storage switchover script

Element	Description
Script Path	Enter the following script path: <code>/u01/app/oracle/admin/bi_ instance/sgstoragescripts/switchvertobisystem2.sh</code>
Target Host	Select STBYBI1.
Script Type	Enter Storage-Switchover as the script type.
Operation Type	Specify Switchover as the operation type.
Credential Type	Specify Privileged Host Credentials as the credential type.

Storage failover script

Element	Description
Script Path	Enter the following script path: <code>/u01/app/oracle/admin/bi_ instance/sgstoragescripts/failovertobisystem2.sh</code>

Element	Description
Target Host	Select STBYBI1.
Script Type	Enter Storage-Failover as the script type.
Operation Type	Specify Failover as the operation type.
Credential Type	Specify Privileged Host Credentials as the credential type.

31.9.2 Associating Storage Scripts for Oracle Business Intelligence Sites Using EMCLI Commands

You must create storage scripts, as described in ["Creating Storage Scripts"](#) and then complete the following:

- [Storage Switchover Script for BISystem1](#)
- [Storage Switchover Script for BISystem2](#)
- [Storage Failover Script for BISystem1](#)
- [Storage Failover Script for BISystem2](#)

Storage Switchover Script for BISystem1

Associate a storage switchover script for BISystem1 by running the following emcli commands in the command-line interface:

```
emcli create_siteguard_script
    -system_name= "BISystem1 "
    -operation="Switchover"
    -script_type="Storage-Switchover"
    -path="/u01/app/oracle/admin/bi_
instance/sgstoragescripts/switchovertobisystem1.sh"
    -host_name="BIHOST1"
    -credential_type="HostPrivileged"
```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

Storage Switchover Script for BISystem2

Associate a storage switchover script for BISystem2 by running the following emcli commands in the command-line interface:

```
emcli create_siteguard_script
    -system_name= "BISystem2 "
    -operation="Switchover"
    -script_type="Storage-Switchover"
    -path="/u01/app/oracle/admin/bi_
instance/sgstoragescripts/switchovertobisystem2.sh"
    -host_name="STBYBI1"
    -credential_type="HostPrivileged"
```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

Storage Failover Script for BISystem1

Associate a storage failover script for BISystem1 by running the following emcli commands in the command-line interface:

```
emcli create_siteguard_script
    -system_name= "BISystem1 "
    -operation="Failover"
```

```

-script_type="Storage-Failover
-path="/u01/app/oracle/admin/bi_
instance/sgstoragescripts/failovertobisystem1.sh"
-host_name="BIHOST1"
-credential_type="HostPrivileged"

```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

Storage Failover Script for BISystem2

Associate a storage failover script for BISystem2 by running the following `emcli` commands in the command-line interface:

```

emcli create_siteguard_script
-system_name= "BISystem2"
-operation="Failover"
-script_type="Storage-Failover"
-path="/u01/app/oracle/admin/bi_
instance/sgstoragescripts/failovertobisystem2.sh"
-host_name="STBYBI1"
-credential_type="HostPrivileged"

```

See [Appendix F.5, "create_siteguard_script"](#) for more information.

31.10 Task 10: Creating Operation Plans

You must create the following operation plans:

- [Operation Plan for Start Operation on BISystem1](#)
- [Operation Plan for Stop Operation on BISystem1](#)
- [Operation Plan for Start Operation on BISystem2](#)
- [Operation Plan for Stop Operation on BISystem2](#)
- [Operation Plan for Switchover Operation on BISystem2](#)
- [Operation Plan for Switchover Operation on BISystem1](#)
- [Operation Plan for Failover Operation on BISystem2](#)
- [Operation Plan for Failover Operation on BISystem1](#)

For more information, see [Executing Oracle Site Guard Operations](#).

Operation Plan for Start Operation on BISystem1

Create a start operation plan by running the following `emcli` commands in the command-line interface:

```

emcli create_operation_plans
_system_name="BISystem1"
-operation="Start"
-name="start-bisystem1"
-role="Primary"

```

See [Appendix F.2, "create_operation_plan"](#) for more information.

Operation Plan for Stop Operation on BISystem1

Create a stop operation plan by running the following `emcli` commands in the command-line interface:

```

emcli create_operation_plan

```

```
-system_name="BISystem1"  
-operation="Stop"  
-name="stop-bisystem1"  
-role="Primary"
```

See [Appendix F.2, "create_operation_plan"](#) for more information.

Operation Plan for Start Operation on BISystem2

Create a start operation plan by running the following `emcli` commands in the command-line interface:

```
emcli create_operation_plan  
-system_name="BISystem2"  
-operation="Start"  
-name="start-bisystem2"  
-role="Standby"
```

See [Appendix F.2, "create_operation_plan"](#) for more information.

Operation Plan for Stop Operation on BISystem2

Create a stop operation plan by running the following `emcli` commands in the command-line interface:

```
emcli create_operation_plan  
-system_name="BISystem2"  
-operation="Stop"  
-name="stop-bisystem2"  
-role="Standby"
```

See [Appendix F.2, "create_operation_plan"](#) for more information.

Operation Plan for Switchover Operation on BISystem2

Create a switchover operation plan by running the following `emcli` commands in the command-line interface:

```
emcli create_operation_plan  
-primary_system_name="BISystem1"  
-standby_system_name="BISystem2"  
-operation="Switchover"  
-name="switchover-to-bisystem2"
```

See [Appendix F.2, "create_operation_plan"](#) for more information.

Operation Plan for Switchover Operation on BISystem1

Create a switchover operation plan by running the following `emcli` commands in the command-line interface:

```
emcli create_operation_plan  
-primary_system_name="BISystem2"  
-standby_system_name="BISystem1"  
-operation="Switchover"  
-name="switchover-to-bisystem1"
```

See [Appendix F.2, "create_operation_plan"](#) for more information.

Operation Plan for Failover Operation on BISystem2

Create a failover operation plan by running the following `emcli` commands in the command-line interface:


```
emcli create_operation_plan
  -primary_system_name="BISystem1"
  -standby_system_name="BISystem2"
  -operation="Failover"
  -name="Failover-to-bisystem2"
```

See [Appendix F.2, "create_operation_plan"](#) for more information.

Operation Plan for Failover Operation on BISystem1

Create a failover operation plan by running the following `emcli` commands in the command-line interface:

```
emcli create_operation_plan
  -primary_system_name="BISystem2"
  -standby_system_name="BISystem1"
  -operation="Failover"
  -name="Failover-to-bisystem1"
```

See [Appendix F.2, "create_operation_plan"](#) for more information.

Listing Operation Plan

To list all operation plans, run the following `emcli` commands in the command-line interface:

```
emcli get_operation_plan
  -name="plan_name"
```

[Figure 31–5](#) shows an example of all operation plans for BISystem1 and BISystem2.

Figure 31–5 Operation Plans for BISystem1 and BISystem2

```
emcli get_operation_plans

Plan Name                                Operation
start-bisystem2                          Start
start-bisystem1                          Start
stop-bisystem1                           Stop
stop-bisystem2                           Stop
switchover-to-bisystem2                  Switchover
switchover-to-bisystem1                  Switchover
failover-to-bisystem1                    Failover
failover-to-bisystem2                    Failover
```

Listing Operation Plan Detail

To obtain information about an operation plan, run the following `emcli` commands in the command-line interface:

```
emcli get_operation_plan_details
  -name="plan_name"
```

See [Appendix F.11, "get_operation_plan_details"](#) for more information.

31.11 Task 11: Starting BISystem1

Start BISystem1 by submitting the `start-bisystem1` operation using `emcli` commands in the command-line interface:

```
emcli submit_operation_plan
  -name="start-bisystem1"
```

See [Appendix F.18, "submit_operation_plan"](#) for more information.

Figure 31–6 shows the start-bisystem1 operation status.

Figure 31–6 Start Status

```
emcli submit_operation_plan -name="start-bisystem1"
Operation plan start-bisystem1 submitted successfully. Please check the Enterprise Manager Grid Control Console for status
```

You can also monitor the status from the Enterprise Manager Cloud Control console by completing the following steps:

1. Log in to Enterprise Manager Cloud Control Console as an EM_CLOUD_ADMINISTRATOR user.
2. Click **Enterprise > Provisioning and Patching > Procedure Activity**.
The **Provisioning** page is displayed.
3. Click the **Procedure Activity** tab.

31.12 Task 12: Stopping BISystem1

Stop BISystem1 by submitting the stop-bisystem1 operation using emcli commands in the command-line interface:

```
emcli submit_operation_plan
      -name="stop-bisystem1"
```

See [Appendix F.18, "submit_operation_plan"](#) for more information.

Figure 31–7 shows the stop-bisystem1 operation status.

Figure 31–7 Stop Status

```
emcli submit_operation_plan -name="stop-bisystem1"
Operation plan stop-bisystem1 submitted successfully. Please check the Enterprise Manager Grid Control Console for status
```

31.13 Task 13: Running the Oracle Site Guard Pre-Check Utility

Oracle Site Guard runs the pre-check utility after you submit the operation plan.

To run the pre-check utility for an operation plan, run the following emcli commands in the command-line interface:

```
emcli run_prechecks
      -operation_plan="name"
```

See [Appendix F.17, "run_prechecks"](#) for more information.

Figure 31–8 shows an example of a pre-check utility emcli command in the command-line interface.

Figure 31–8 Pre-Check Utility

```
emcli run_prechecks -operation_plan="switchover-to-bisystem2"
Prechecks for operation plan switchover-to-bisystem2 submitted successfully. Please check the Enterprise Manager Grid Control Console for status
```

31.14 Task 14: Performing Site Switchover

You must complete the following:

- [Switchover to BISystem1](#)
- [Switchover to BISystem2](#)

Switchover to BISystem1

To perform a site switchover to BISystem1, run the following emcli commands in the command-line interface:

```
emcli submit_operation_plan
      -name="switchover-to-bisystem1"
```

See [Appendix F.18, "submit_operation_plan"](#) for more information.

[Figure 31–9](#) shows the switchover operation status.

Figure 31–9 Switchover Status for BISystem1

```
emcli submit_operation_plan -name="switchover-to-bisystem1"
operation plan switchover-to-bisystem1 submitted successfully. Please check the Enterprise Manager Grid Control Console for s
```

Switchover to BISystem2

To perform a site switchover to BISystem2, run the following emcli commands in the command-line interface:

```
emcli submit_operation_plan
      -name="switchover-to-bisystem2"
```

See [Appendix F.18, "submit_operation_plan"](#) for more information.

[Figure 31–10](#) shows the switchover operation status.

Figure 31–10 Switchover Status for BISystem2

```
emcli submit_operation_plan -name="switchover-to-bisystem2"
operation plan switchover-to-bisystem2 submitted successfully. Please check the Enterprise Manager Grid Control Console for s
```

After you perform switchover the associations in the Site Guard configuration will be updated, as shown in [Figure 31–11](#).

Figure 31–11 Updated Site Guard Status

```
emcli get_siteguard_configuration
Primary System      Standby System(s)
BISystem2          BISystem1
```

31.15 Task 15: Performing Site Failover

To perform a site failover, complete the following steps:

- [Failover to BISystem1](#)
- [Failover to BISystem2](#)

Failover to BISystem1

To perform a site failover to BISystem1, run the following emcli commands in the command-line interface:

```
emcli submit_operation_plan
```

```
-name="failover-to-bisystem1"
```

See [Appendix F.18, "submit_operation_plan"](#) for more information.

[Figure 31–12](#) shows the failover operation status.

Figure 31–12 Failover Status for BISystem1

```
emcli submit_operation_plan -name="failover-to-bisystem1"  
operation plan failover-to-bisystem1 submitted successfully. Please check the Enterprise Manager Grid Control Console for status
```

Failover to BISystem2

To perform a site failover to BISystem2, run the following emcli commands in the command-line interface:

```
emcli submit_operation_plan  
-name="failover-to-bisystem2"
```

See [Appendix F.18, "submit_operation_plan"](#) for more information.

[Figure 31–13](#) shows the failover operation status.

Figure 31–13 Failover Status for BISystem2

```
emcli submit_operation_plan -name="failover-to-bisystem2"  
operation plan failover-to-bisystem2 submitted successfully. Please check the Enterprise Manager Grid Control Console for status
```

Part X

Deployment Procedures

This part contains the following chapters:

- [Chapter 32, "About Deployment Procedures"](#)
- [Chapter 33, "Customizing Deployment Procedures"](#)

About Deployment Procedures

This chapter provides an overview of Deployment Procedures and describes the key aspects you need to know about them. In particular, this chapter covers the following:

- [Overview of the Procedure Management Solution](#)
- [Granting Roles and Privileges to Administrators](#)
- [Components of a Procedure](#)
- [Creating, Saving, and Launching User Defined Deployment Procedure \(UDDP\)](#)
- [Managing Deployment Procedures](#)
- [Executing Procedure Instance Tasks](#)

32.1 Overview of the Procedure Management Solution

This section describes the following:

- [Overview of the Provisioning Page](#)
- [Comparison Between the Existing Design and the New Design for Procedure Instance Execution Page](#)
- [Overview of the New Procedure Instance Execution Page](#)

32.1.1 Overview of the Provisioning Page

Enterprise Manager provides a framework for automating, orchestrating, and tracking tasks that can be run on multiple Oracle homes. You can perform complex software life cycle management activities such as provisioning, patching, upgrade, and so on from the Cloud Control console. The workflow of all the tasks that need to be performed for a particular life cycle management activity is encapsulated in a Procedure. A Procedure is a hierarchal sequence of provisioning steps, where each step may contain a sequence of other steps. It provides a framework where specific applications and procedures can be built.

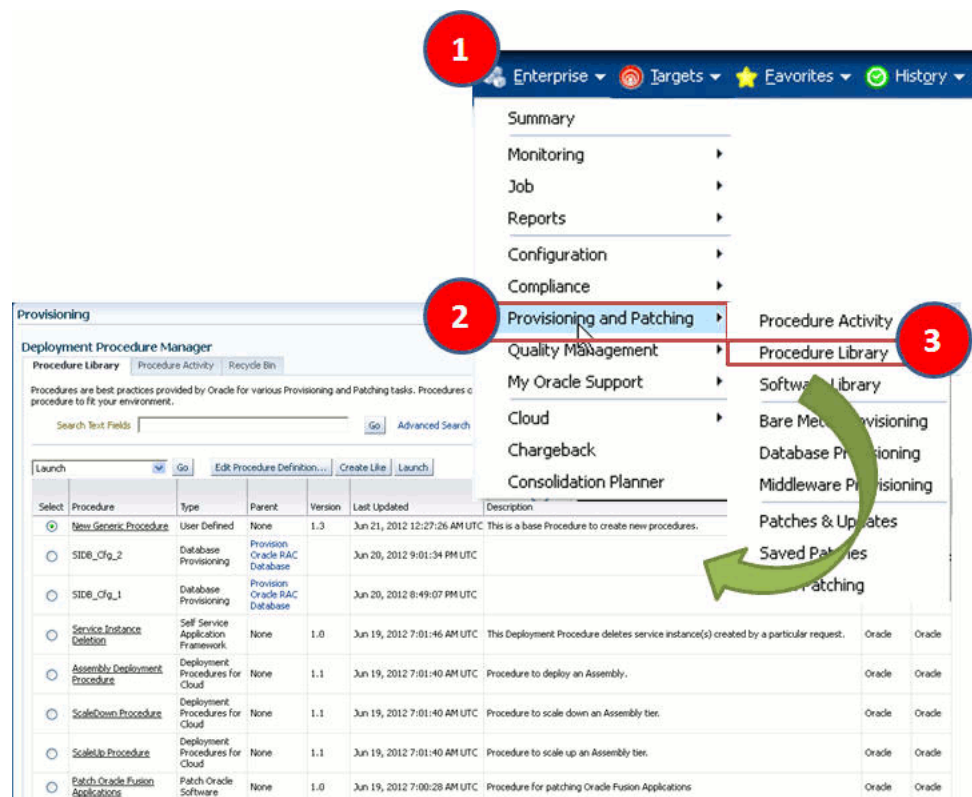
Oracle Enterprise Manager Cloud Control (Cloud Control) comes with a set of default Procedures that help you accomplish common provisioning and patching-related tasks. Each Procedure is unique, and is designed to perform a particular operation according to the source being provisioned or target being patched. For example, the Procedure to patch a single instance database differs from the one to patch an Oracle RAC environment or an application server.

The Provisioning page has three tabs: Procedure Library, Procedure Activity, and Recycle Bin.

- **Procedure Library Tab:** This tab lists all available procedures. Procedures created by Oracle Corporation cannot be edited or deleted. For information about the tasks that can be performed from the Procedure Library page, refer to [Section 32.5](#).
- **Procedure Activity Tab:** This tab lists all the procedures that have been submitted to be executed. Currently, after a procedure is submitted, you can track the instance in a couple of ways, for details refer to [Table 32-1](#).
- **Recycle Bin Tab:** You can delete procedures and runs. When procedures or runs are deleted, they will be internally marked as deleted and will be displayed in the Recycle Bin tab.

[Figure 32-1](#) shows you how you can access the Provisioning screen from within Cloud Control.

Figure 32-1 Accessing the Provisioning Page



32.1.2 Comparison Between the Existing Design and the New Design for Procedure Instance Execution Page

The current Procedure Activity page provides the status of all the steps executed in a deployment procedure. This page also gives you information of the failed step and the necessary action to be taken to rectify it.

Before you understand the new Procedure Activity page, take a moment to review the challenges you might be facing while using the current Procedure Activity Page:

Table 32–1 Comparison Between the Existing Procedure Activity Page and the New Procedure Activity Page.

Category	Existing Procedure Activity Page	New Procedure Activity Page
Screen Design	The screen design allows you to access one step at a time.	Optimal screen design which allows you to access all the steps and targets from the same page without having to drill down
Multiple Selects	Multiple selects are not supported.	Multiple selects are possible from a single page. For example, if you want to select only the failed steps you can do so using the new design.
Target-Centric Design	Step-centric approach restricts your access to all the targets from a single screen. Which means that in the earlier approach you could drill down to only one failed step at a time, and would have to repeat the whole procedure for the other failed steps	Target-centric design with the introduction of filters have made it easy to analyze all failed steps from the same page and perform the required action on the step.
Step Output	The step-centric design requires traversing through a number of pages to drill down to the actual step.	Target-centric design now allows you to view all the step details from the same page. unlike the earlier step-centric.
Detailed Output	Detailed Output for a step was not available in the earlier design. You had to download the entire log.	Detailed Output is a new option available at step-level which captures the log information pertaining to that step selected, only making it easy to view and debug the step in case of a failure.
Incident Creation	Incident Creation was not available in the earlier design.	Incident Creation is a new feature that has been introduced at Procedure-Level which enables you to create an incident for the execution which can later be used to debug the procedure in case of a failure.

Note: Enterprise Manager provides you the flexibility of switching between the Existing Procedure Activity Page and the New Procedure Activity Page. To do so, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, select **Procedure Activity**.
2. On the Deployment Procedure Manager page, select the procedure.
3. On the Procedure Activity page, click **Switch to Classic View** to go back to the Existing Procedure Activity Page.

To switch to the New Procedure Activity Page, click **Switch to Advanced View**.

Cloud Control addresses the challenges of the existing Procedure Activity page with its much-improved target-centric procedure management solution that allows access

to all the targets and steps from one single page with maximum ease and minimum time. The new Procedure Activity page offers the following benefits

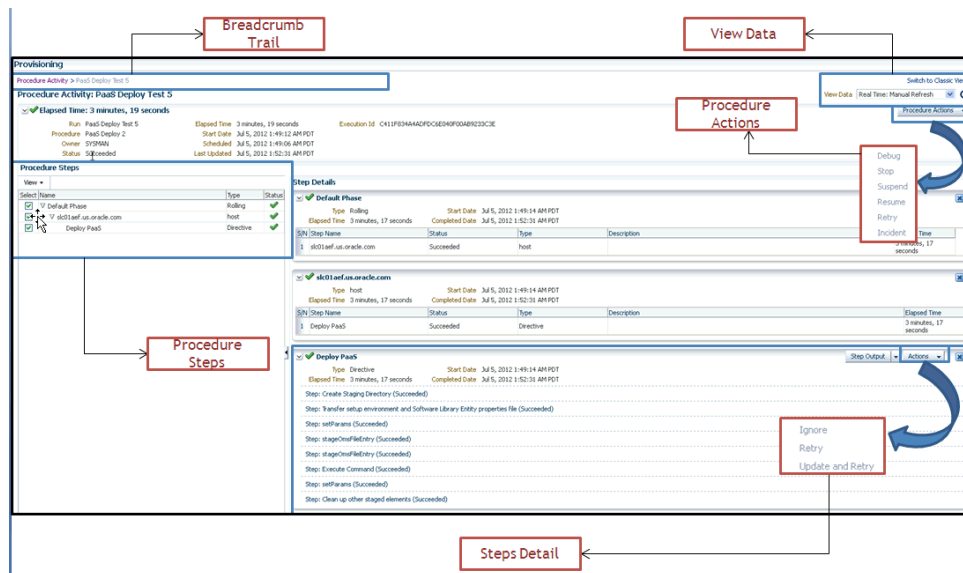
32.1.3 Overview of the New Procedure Instance Execution Page

The Procedure Activity page primarily helps you track the execution of the procedure instance submitted. Click any instance running to view the new Procedure Instance Execution page which is broadly divided into the following regions as shown in Figure 32–2:

- [Breadcrumb Trail](#)
- [View Data](#)
- [Procedure Summary Section](#)
- [Procedure Steps Section](#)
- [Step Details Section](#)

Note: For information about the tasks that can be performed from the Procedure Instance Execution Page, refer to [Section 32.6](#).

Figure 32–2 Procedure Execution Page



Breadcrumb Trail

Enables you to go back to the Procedure Activity page with a single click.

View Data

Enables you to refresh the page after making some procedure-level or step-level updates. To do so, you must select the refresh options available in the **View Data** menu. To run the procedure refresh in the background, you can select any of the auto refresh options like: **30 seconds Refresh**, **1 minute Refresh**, or **5 minute Refresh** and continue to work on other areas.

Procedure Summary Section

Enables you to display the instance execution details like execution name, the procedure name, the owner of the procedure, the status of the procedure, the start date, the time elapsed since the procedure started, the scheduled time for the procedure execution, the last time the procedure was updated, the execution ID of the procedure, and the last filed incident if any. The details in this section are mostly static except for the **Elapsed Time** field which is constantly updated till the procedure is running.

If the procedure has successfully completed with a status **Succeeded**, then the Procedure Actions menu items are greyed out, you can not perform any actions on a successful procedure. However, if the procedure was stopped or suspended for some reason, then corresponding menu items are enabled so that you can control the procedure execution.

At Procedure-level, you can perform the following actions:

Action	Description
Debug	Debugs the errors in the procedure. This is a one time action, which means that the menu is disabled after using this option the first time.
Stop	Stops the procedure execution.
Suspend	Suspends the procedure execution.
Resume	Resumes the procedure from the stage it was stopped or suspended.
Retry	Executes all the failed steps and phases in the deployment procedure instance once again.
Incident	Creates an incident for the execution which enables you to debug / understand all the steps and phases executed as a part of the deployment procedure.

Procedure Steps Section

Enables you to view all the steps that are run when the procedure instance is submitted for execution. From the **View** menu, select **Expand All** to view the step details like: step name, the type of step, and the status of the step.

For example, if the first step is a computational step called "Initialize Deployment Procedure". When this step is selected, its corresponding execution details are displayed in the Execution Details section. If the step has failed, then you can select the action you want to perform on the step from the **Actions** menu.

Step Details Section

Enables you to view the details of the selected step. Essentially, information like Step Type, Start date, Completed Date, and Elapsed Time for the step is displayed. However, the template for each step type is not the same. For example, the manual step requires user intervention, which means you might need to confirm some details for the job to proceed. Closing the step window, deselects the step from the Procedure Steps section.

The Detailed Output option allows you to view the log information for the selected step provided it has completed execution successfully.

Note: If a step has failed to complete execution or if a step is of type host or manual, then the Detailed Output option is not displayed in the Step Details section.

If a step has failed, then you can perform the following actions on the step using the Actions menu:

Action	Description
Ignore	Ignore the failure of a step, and continue with the other steps in the deployment procedure.
Retry	Executes the step once again
Update and Retry	Enables you to edit the step, and then executes the step when submitted.

32.2 Granting Roles and Privileges to Administrators

Administrators are Enterprise Manager users who can login to Enterprise Manager to perform management tasks. The breadth of management tasks available in Enterprise Manager depends on the privileges and roles assigned to the administrators. Roles allow grouping of Enterprise Manager secure resource privileges and can be granted to administrators or to other roles. Based on the roles, and privileges granted to an Administrator, they can be broadly classified into Designers, and Operators. Normally, the roles and privileges are granted to users or other roles at deployment procedure level, and Software Library level.

This section describes how administrators are granted the predefined roles and privileges that Oracle provides:

- [Granting Roles and Privileges to Administrators on the Deployment Procedure](#)
- [Granting Roles and Privileges to Administrators on Software Library](#)

32.2.1 Granting Roles and Privileges to Administrators on the Deployment Procedure

In a typical data center, the main users of Deployment Procedures are Designers (Lead Administrators) and Operators. Deployment Procedure privileges enable users to perform some design-time activities like setting Privilege Delegation, customizing Deployment Procedure, and run-time activities like running the Deployment Procedure to provision or patch software applications.

Following are the primary users/roles predefined by Oracle for a Deployment procedure, and their associated privileges:

- Super Administrator role allows you to perform all the Administrative operations, and provides full privileges on all the targets.
- `EM_ALL_DESIGNER` (Designer): This role allows you to perform design time operations on entities. For example, Creating and Monitoring Deployment Procedure templates.

The following table lists all the roles predefined for Designers, and their corresponding descriptions:

Table 32–2 Predefined Roles for Designers

Roles	Description
EM_PATCH_DESIGNER	Role has privileges for creating and viewing any patch plan
EM_PROVISIONING_DESIGNER	Role has privileges for provisioning designer
EM_TC_DESIGNER	Role has privileges for creating Template Collections

Users can be granted any of the following Target Privileges:

- Create Privilege Propagating Group. Privileges granted on a privilege propagating group will be automatically granted to the members of the group.
- Add any target in Enterprise Manager.

Users can be granted any of the following Resource Privileges:

- Create Compliance Entity.
- Create Enterprise Rule Set, basically collection of rules that apply to Enterprise Manager elements, for example, targets and job.
- Create Metric Extension. Metric Extensions allows extending monitoring for a target type by adding new metrics.
- Create new Named Credential that are required to perform Enterprise Manager Administrative Operations.
- Create Any Software Library Entity, Import Any Software Library Entity, Export Any Software Library Entity, and so on.
- Create Template Collection.

Note: For information about EM_PATCH_DESIGNER see [Table 24–3](#), and for information about EM_PROVISIONING_DESIGNER see [Table 4–3](#).

- EM_ALL_OPERATOR (Operator): This role has restricted access, and allows you to perform only the run-time activities. For example, Launching a Deployment Procedure.

The following table lists all the roles predefined for Operators, and their corresponding descriptions:

Table 32–3 Predefined Roles for Operators

Roles	Description
EM_ALL_VIEWER	Role Desc
EM_HOST_DISCOVERY_OPERATOR	Role has privileges to execute host discovery
EM_PATCH_OPERATOR	Role for deploying patch plans
EM_PROVISIONING_OPERATOR	Role has privileges for provisioning operator
EM_TARGET_DISCOVERY_OPERATOR	Role has privileges to execute target discovery
EM_USER	Role Desc

Users can be granted any of the following Target Privileges:

- Connect and manage any of the viewable target.
- Add any target in Enterprise Manager.
- Perform administrative operations on all managed targets
- Run any Operating System Command at any Management Agent

Users can be granted any of the following Resource Privileges:

- Application Replay Operator. Application Replay Entities include captures, replay tasks, and replays.
- Manage custom configurations owned by the user
- Create new Named Credential that are required to perform Enterprise Manager Administrative Operations.

Note: For information about `EM_PATCH_OPERATOR` see [Table 24–3](#), and for information about `EM_PROVISIONING_OPERATOR` see [Table 4–3](#).

32.2.2 Granting Roles and Privileges to Administrators on Software Library

Software Library is a centralized media storage for all Enterprise Manager entities. Super Administrator is responsible for configuring the Software Library, once the Enterprise Manager installation is complete. After the Software Library is configured with Storage Locations, it becomes usable to store entities. Designers and Operators are the main users of Software Library who perform the design-time and run-time activities respectively. The design-time activities include Customizing entities, Creating entities, Importing entities, Exporting entities, and so on. The run-time activities performed by Operators include running deployment procedures which in turn use any the entities stored in the Software Library.

For more information about Software Library users, roles, and their associates privileges, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Note: To run the procedure on a Windows host which involves executing some Software Library entities (for example, directive scripts), you (*the Windows user*) must be granted the following privileges:

- Act as part of the operating system
- Adjust memory quotas for a process
- Logon as batch job
- Replace a process level token

If not, the execution of the directive steps in the procedure may fail.

32.3 Components of a Procedure

This section describes the following:

- [Target List](#)
- [Procedure Variables](#)
- [Phases and Steps](#)

32.3.1 Target List

Target List is a pre-populated list of targets on which you can run your job. Phases operate on a set of Enterprise Manager targets, collectively known as a target list. Each phase must be associated with a target list. When the Deployment Procedure is selected for execution, the Deployment Procedure Manager will prompt the user to assign targets to the target list.

Starting with Enterprise Manager 12c (12.1.0.2), Custom Target Lists have been introduced. In addition to the default target list, you can now have your own customized lists of targets on which designated Phases can run. The advantage of this approach is that you can have multiple custom target lists, and assign it to the different phases in your procedure. This allows you to choose the Target List on which you want the Phase to iterate.

The following examples describes the various scenarios which employs one, two, or more target lists in a procedure:

- For copying a jar file to multiple hosts, you will need just one target list. You may choose to use the default target list for this purpose.
- For cloning an Oracle Home, and provisioning it on multiple targets, you will need a minimum of two target lists: one target list for the source which contains only a single target, and a second target list which contains all the destination targets.
- For provisioning or patching a WebLogic Server, you might require three separate target lists one for the Administration Server, one for the Managed Servers, and one for the Database.

32.3.2 Procedure Variables

Procedure Variables are user-defined variables that can be used while customizing a procedure. Normally, when you add a custom step to a User-owned procedure or customize an Oracle-owned procedure, then you might need to declare procedure variables that you can later use in your custom step or phase.

To access the Procedure Variable tab, from the **Enterprise** menu, select **Provisioning and Patching** and then select **Procedure Library**. On Provisioning page, select a Deployment Procedure, and click **Create Like**. A page similar to the following appears:

Select	Name	Display Name	Description	Password	Required
<input type="radio"/>	DBVER	database version	version of the database	<input type="checkbox"/>	<input type="checkbox"/>

To declare the Procedure Variable, you must enter a unique name, a description for it. Optionally, you can select the password check box to make the variable secure.

You can create two types of Procedure Variables that can be later used while launching the deployment procedure. They are as follows:

- **String:** This variable once declared at design-time, can be used by operator to specify the values at run time. For example, DBVER (the version of the database).

- Software Library Entity:** This variable allows you the flexibility of binding the variable to Software Library Directive or Component at the time of launching the procedure. Earlier these values had to be specified at design-time while creating the procedure, now with the introduction of Software Library entity variable you can specify the values dynamically at the time of launching the procedure.

For information about adding Software Library variables, see [Section 33.2.1.4](#) or [Section 33.2.1.3](#).

Note: You cannot add Procedure Variables to a Deployment Procedure that is owned by Oracle.

32.3.3 Phases and Steps

Deployment Procedures comprise various phases and steps that run serially or in parallel to perform a particular provisioning or patching operation.

A phase contains steps or more phases. The different types of phases are:

- Rolling Phase*

Rolling phase is a phase where steps are run serially across targets.

▽ For all unique RAC databases	Rolling	Iterates over each unique RAC database running from distinct oracle home directory
▽ For all hosts	Rolling	Iterates over a list of hosts.
▽ For all homes	Rolling	Iterates over a list of Oracle Homes.

- Parallel Phase*

Parallel phase is a phase where steps are run in parallel across targets.

▽ For all unique Cluster ASMs	Parallel	Iterates over each unique Cluster ASM instances running from distinct oracle home directory
▽ For all hosts	Parallel	Iterates over a list of hosts.

A step is an abstraction of a unit of work. For example, starting the database is a step. It is either part of a phase or independent. The different types of steps are:

- Manual Step*

Manual Step is that task that requires user interaction and cannot be automated. Typically, Deployment Manager would display the instructions that need to be performed by the user. After the operation is performed, the user proceeds to the next step.

Examples of a Manual Step:

- Log on to a system and update the kernel parameter.
- Reboot a system.
- Provide special privileges to the user. For example, SSH Setup.

Pause after prerequisite checks	Manual	The deployment procedure instance has performed the prerequisite checks and is currently paused for you to examine the results and proceed. Review the prerequisite results and then proceed with the deployment.
---------------------------------	--------	---

- Computational Step*

Computational Step is that task whose operations are performed within the Deployment Engine and does not require any user intervention. This step gathers additional information for executing a procedure. This step cannot be inserted by a user, and only Oracle Corporation can insert this step.

Examples of Computational Step:

- Executing SQL query against an Enterprise Manager schema to gather more data for other steps to run.
- Retrieving target properties from the repository and updating the runtime information.

Patch Oracle RAC Database - All Nodes		Procedure for patching an Oracle RAC Database (supports application of patchsets too). This procedure patches Oracle Home RAC Database installations. All selected instances are patched in parallel. This procedure patches installations registered with different clusterware. Applicable for version 10.1, 10.2 and higher. Note: Migration from 10.1 to 10.2 is not supported.
<u>Initialize</u>	Computational	Initializes runtime data. Also downloads patches from My Oracle Support and creates software library components you have selected to run from My Oracle Support.
<u>Check for Supported Configurations</u>	Computational	Does a set of checks to validate if the targets are supported for patching.
<u>Check for Target Properties</u>	Computational	Verifies whether all the required target properties are present and whether the associations are proper.

- *File Transfer Step*

File Transfer Step is a step used for copying files and/or directories from one host to one or more hosts. You can archive files and directories transferred from a source host to the destination hosts. When this step is inserted within a phase, you can set the Source and Destination Targets using existing variables.

For example, to copy a directory from a host X to the hosts associated with the phase, then for Source Target select "Set Value" and assign host X, and for Destination Target select "Choose Variable" and assign it to the option "TargetVariable:Current Target".

<u>Copy Grid Infrastructure Archive</u>	File Transfer	Copies the Grid Infrastructure archive from the reference host to the destination hosts that require Grid Infrastructure Oracle home for provisioning.
---	---------------	--

- *Action Step*

Action step is a task that performs some operations run on one or more targets. They must be enclosed within a phase. The Deployment Procedure maps the Action Step and target pair to a job in the Enterprise Manager Job System. The Deployment Procedure can schedule, submit, and run a job per Action Step per target. For example, running a script, applying a patch, upgrading an Oracle home, and so on.

Also note that an Action Step is said to have completed successfully only when all its associated jobs have completed successfully. If a job fails, then the Action Step also fails. You may then manually restart the job in question or ignore and instruct the Deployment Procedure to proceed.

The different types of Action Steps include:

- *Job*

Job Step is a special type of Action Step that executes a predefined job type on a target. This is used if you want to execute a job type as a part of a Deployment Procedure. You need to pass job parameters for a step.

Examples of Job Step:

- * Cloning an existing Oracle home.
- * Staging a patch.
- * Starting a database.

Upgrade OPatch	Job	Upgrades OPatch to the latest version.
Stage Patches	Job	Stages the selected patches to Oracle homes. For example, %emd_root%/EMStagedPatches. Ensure that you have read and write permissions in the staging location.
Stage OUI and OPatch	Job	Stages OUI and OPatch to Oracle homes if required. For example, %emd_root%/EMStagedPatches. Ensure that you have read and write permissions in the staging location.

– *Library: Directive*

Directive Step is a special type of Action Step to deploy a directive alone. This is useful when users want to store their custom scripts in the Software Library and reuse them in a Deployment Procedure.

For more information about Directives, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Examples of Directive Step:

- * Executing root scripts.
- * Applying `catpatch.sql` and restarting the database.
- * Confirming if the prerequisites have been met.

For all homes	Rolling	Iterates over a list of Oracle Homes.
Check Home Normal Credentials	Directive	Verifies the credentials of the Oracle home.
Check Home Privilege Credentials	Directive	Verifies the super user privileged credentials of the Oracle home.
Check for Target Status	Directive	Verifies the target tools, commands, and permissions.

– *Library: Component*

A Component Step is a special type of Action Step to deploy a Software Library Component and the associated Directive. Deployment Procedure Manager executes the directive with respect to the component. Components used for Generic Component Step generally has one directive associated with it. This association is done by selecting both the component and directive while creating the step. All directives that you associate with the component while uploading to the software library will be ignored while executing the step.

For more information about Components, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

Examples of Component Step:

- * Applying a patch.
- * Performing prerequisites before performing an installation.
- * Installing Oracle software on target machines.

Check Shared RAC Home	Component	Check whether specified RAC Home is Shared or not.
-----------------------	-----------	--

– *Host Command*

Host Command Step is a special type of Action Step that encapsulates simple host commands. This step allows the user to enter a command line or a script (multiple commands) to be executed on the target host.

Examples of Host Command Step:

- * Starting a Management Agent (`emctl start agent`)

- * Shutting down OPMN (`opmnctl stopall`)
- * Restarting OID

Pre-Stage Custom Host Command Step	Host Command	Custom step to run user commands
---------------------------------------	-----------------	----------------------------------

32.4 Creating, Saving, and Launching User Defined Deployment Procedure (UDDP)

Creating a procedure from scratch by inserting the required phases, steps, variables, and so on is possible with User Defined Deployment Procedure. This functionality has been introduced in Enterprise Manager 12c to allow users to completely customize a procedure to suit their requirements. Broadly the process can be divided into two subcategories as follows:

- [Step 1: Creating User Defined Deployment Procedure](#)
- [Step 2: Saving and Launching User Defined Deployment Procedure with Default Inputs](#)
- [Step 3: Launching and Running the Saved User Defined Deployment Procedure](#)
- [Step 4: Tracking the Submitted User Defined Deployment Procedure](#)

Note: For a workflow example on User Defined Deployment Procedure with illustrations on how to provision JRE6 on a Linux host `abc.example.com`, see [Section A.6.3](#).

32.4.1 Step 1: Creating User Defined Deployment Procedure

Log in to Enterprise Manager Cloud Control with designer privileges to create a UDDP template. To do so, follows these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, select **Procedure Library**.
2. On the Provisioning page, from the list of actions, select **Create New**, and click **Go**.
3. On the Create New Procedure page, in the General Information tab, provide a unique name and description for your procedure.
4. In the Target Lists tab, you can use the default `host_target_list` variable or add any number of new custom target lists. Adding new custom target lists enables you to group the targets which in turn allows phases to use separate target lists (targets) that they can iterate on.
5. In the Procedure Variables tab, click **Add Row** to define procedure variables. In addition to String type, you can add Software Library Entity variable. For more information about this, refer to [Section 32.3.2](#).

Specify the **Variable Name**, **Display Name**, **Description**, and **Type** from the drop down menu. Also define whether the variable is a password and a mandatory field.

6. In the Procedure Steps tab, select the default phase, and do the following:
 - a. Select Default Phase, and click **Insert**. For information on inserting a phase, see [Section 33.2.1.1](#).

Note: Without declaring a Target List, you can not proceed with the creation of a phase.

- b. Select the phase you created, and then click Insert to insert steps. For information on inserting steps, see [Section 33.2.1](#).
7. Repeat steps 6 to insert steps and phases according to the procedure you want to create.
8. Click **Save and Close** to save the procedure. You can run the configuration for future deployments.

32.4.2 Step 2: Saving and Launching User Defined Deployment Procedure with Default Inputs

Log in to Enterprise Manager Cloud Control with Operator privileges to save the saved UDDP with default values. To do so, follows these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, select **Procedure Library**.
2. On the Provisioning page, select the saved UDDP, and click **Launch**.
3. On the Select Targets page, select the target list from the drop down menu, and click **Add** to populate the target list. Click **Next**.
4. If you declared variables that you did not define during the procedure creation, then you will have to provide the details in the Set variable page. All the unbound variables are displayed, enter appropriate values for the same.

If you have declared a Software Library Entity variable, then you could search and select the desired entity from Software Library. Once the value is populated, you may even choose to lock this value so that any other Operator who does not have privileges on your procedure will not be able to update this values. For more information on different types of variables, see [Section 32.3.2](#). Click **Next**.

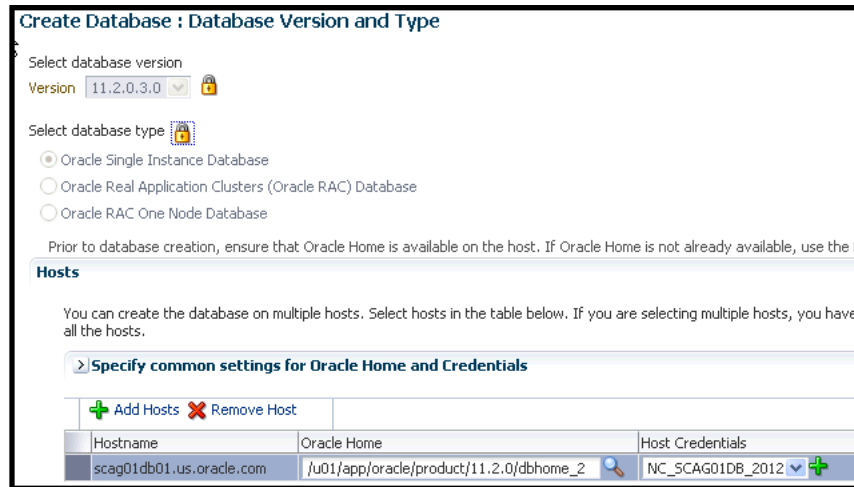
5. On the Set Credentials page, you need to set the credentials for the target host machines that you have included as a part of the `host_target_list` variable. Click **Next**.
6. On the Set Schedule and Notification page, you can schedule the job to run immediately or at a later preferred time.
7. Click **Save**, and provide a configuration name to save the job template with default values.

Some of the procedures allow you to not just save the procedure with default values, but also lock them. For example, the following Database Provisioning procedure describes how to save and launch a procedure with lock downs.

32.4.2.1 Saving and Launching the Deployment Procedure with Lock Down

Lock Down is a new feature introduced in Oracle Enterprise Manager Cloud Control 12c that enables administrators with Designer privileges to standardize the Deployment Procedures across the enterprise. If Designers with Super Administrator privileges create Deployment Procedure templates with lock downs, and save them, then these templates can be used by Operators who can launch the saved Deployment Procedures, make changes to the editable fields, and then run them.

To create a Deployment Procedure with lock downs, an administrator logs in with designer privileges, and launches a Deployment Procedure. In the interview wizard of the Deployment Procedure, the designer enters the values for certain fields and locks them so that they cannot be edited when accessed by other users. For example, in the following graphic, fields like **Database Version**, **Database type** are locked by the designer, and when an operator launches the same deployment procedure, these fields will be grayed out, and cannot be edited:



In the following use case, user logs in with designer privileges to provision a Single Instance Database on a Linux host. *Designer* updates most of the values prompted in the wizard and locks them as he/she does not want other users like Operators to have edit privileges on them. Some of the fields like adding targets, and some additional configuration details are not locked. The Deployment Procedure is then saved with a unique procedure name, but not submitted. A user with *Operator* privileges logs in and runs the saved procedure after updating all the editable fields, like adding targets, additional configuration details.

Broadly, it is a two-step process as follows:

- [Step 1: Saving a Single Instance Database Deployment Procedure with Lock Downs](#)
- [Step 2: Launching the Saved Single Instance Database Deployment Procedure](#)

Step 1: Saving a Single Instance Database Deployment Procedure with Lock Downs

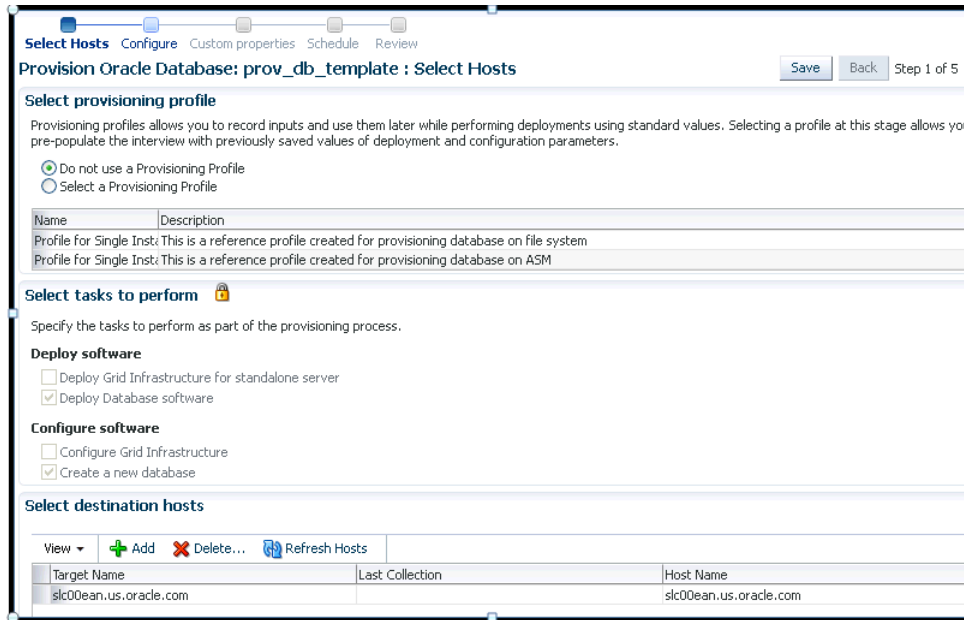
In the following section user logs in to Cloud Control as a designer (ATBARBOZ1), and provisions a Single Instance Database with lock downs as follows:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. On the Database Provisioning page, select **Provision Oracle Database**, and click **Launch**.
3. In the Select Hosts page, in the Select hosts section, click **Add** to select the destination host where you want to deploy and configure the software.

If you want to use a provisioning profile for the deployment, choose **Select a Provisioning Profile** and then select the profile with previously saved configuration parameters.

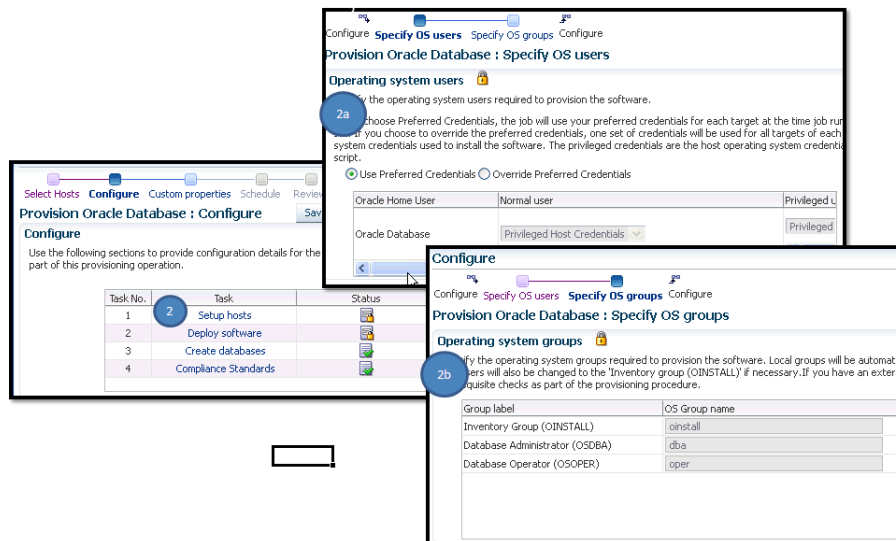
In the Select Tasks to Perform section, do the following and lock the values:

- Select **Deploy Database software** to provision single instance databases
- Select **Create a New Database** to create a new database and configure it after installing the standalone Oracle Database



4. On the Configure page, the following configuration options appear:

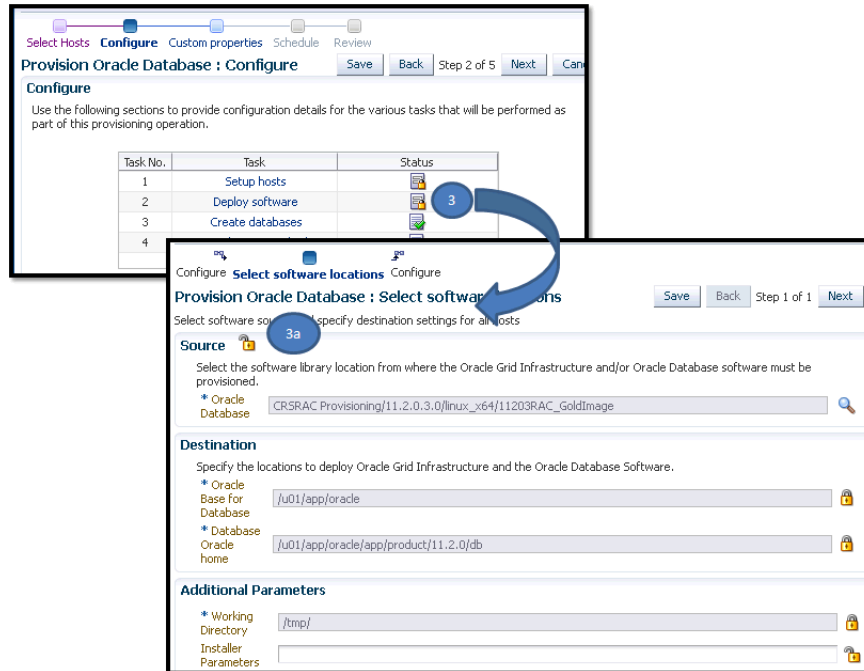
- On the Configure page, click **Setup Hosts**. On the Operating System Users page, specify the operating system user for the Oracle Home for the database. For Oracle Home User for the database, select the Normal User and Privileged User to be added to the OS group, and lock the values. Click **Next** to proceed. On the Specify Operating System groups page, specify the OS Groups to use for operating system authentication and lock the values, as appears in the following graphic



Click **Next** to come back to the Configure page.

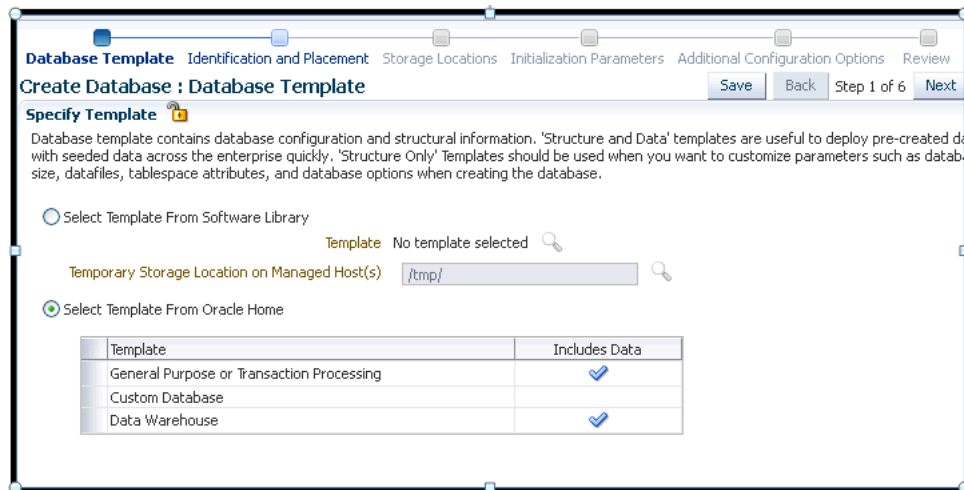
- On the Configure page, click **Deploy Software**. On the Select Software Locations page, specify the source and destination locations for the software

binaries of Oracle Database. Update the values for all the fields, and click the Lock icon so that the fields can not be edited by a user with Operator privileges, as appears in the following graphic:

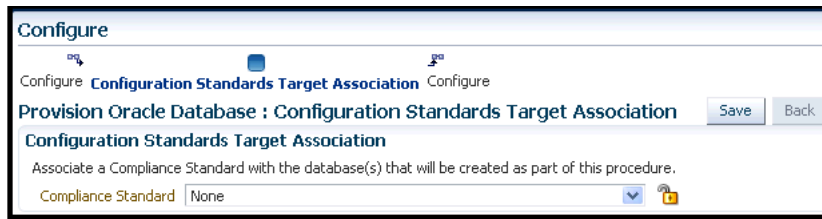


Click **Next** to come back to the Configure page.

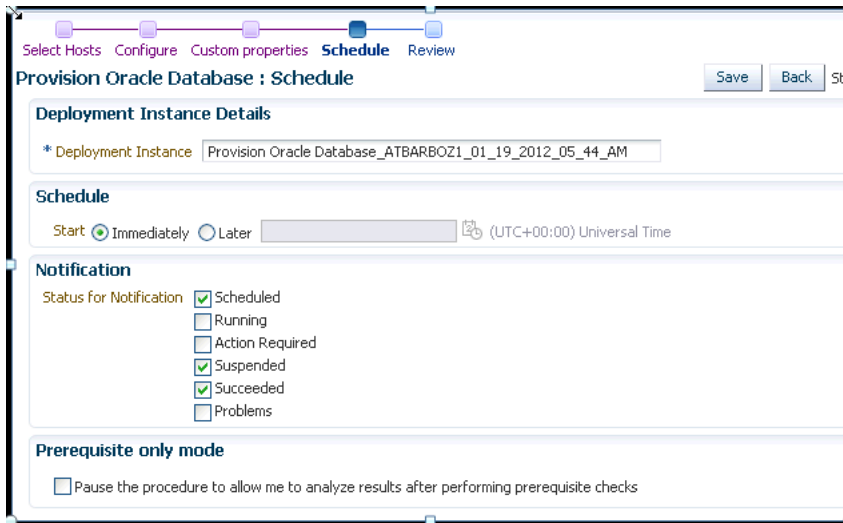
- On the Configure page, click **Create Databases**, the following screen appears. Update only the mandatory fields, and click **Next** to proceed. Do not lock any of the values in this wizard:



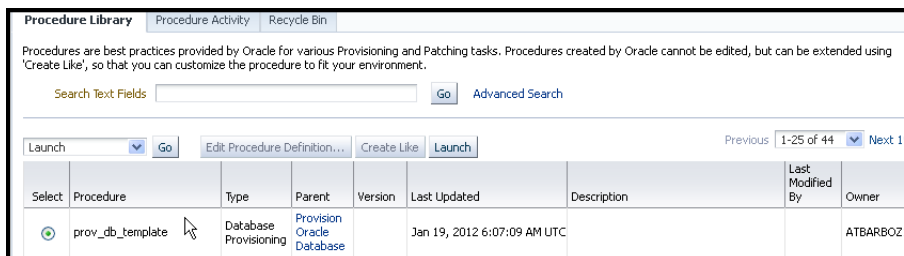
- On the Configure page, click **Compliance Standards**. On the Configuration Standards Target Association page, select a Compliance Standard to be associated with the database. Click **Next**. Do not lock the values.



- On the Schedule page, specify a Deployment Instance name. In the Schedule section, select **Immediately**. You can set the notification preferences according to deployment procedure status, and click **Next**.



- In the Review page, review the details you have provided for the deployment procedure. Click **Save** to save the deployment procedure with a unique name **prov_db_template**, and then click **Cancel**. The Procedure library page appears with the saved procedure



Step 2: Launching the Saved Single Instance Database Deployment Procedure

In the following section user logs in as a Operator (SSIRAJUD1), and runs the saved Deployment Procedure **prov_db_template** to provision a Single Instance Database.

- In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
- In the Procedure Library, select a procedure **prov_db_template**, and click **Launch**.

The screenshot shows the Oracle Enterprise Manager user interface. At the top, there is a user menu with 'Select', 'Help', 'SSIRAJUD1', and 'Log Out'. A blue callout box points to the user name 'SSIRAJUD1' with the text: 'Log in with Operator Privileges SSIRAJUD1 to run a DP owned by the designer ATBARBOZ1.' Below this is a table of deployment procedures:

Select	Procedure	Type	Parent	Version	Last Updated	Description	Last Modified By	Owner
<input checked="" type="radio"/>	prov_db_template	Database Provisioning	Provision Oracle Database		Jan 19, 2012 6:07:09 AM UTC			ATBARBOZ1

- On the Select Hosts page, in the Select hosts section, click **Add** to select the destination host where you want to deploy and configure the software, and then click **Next**.

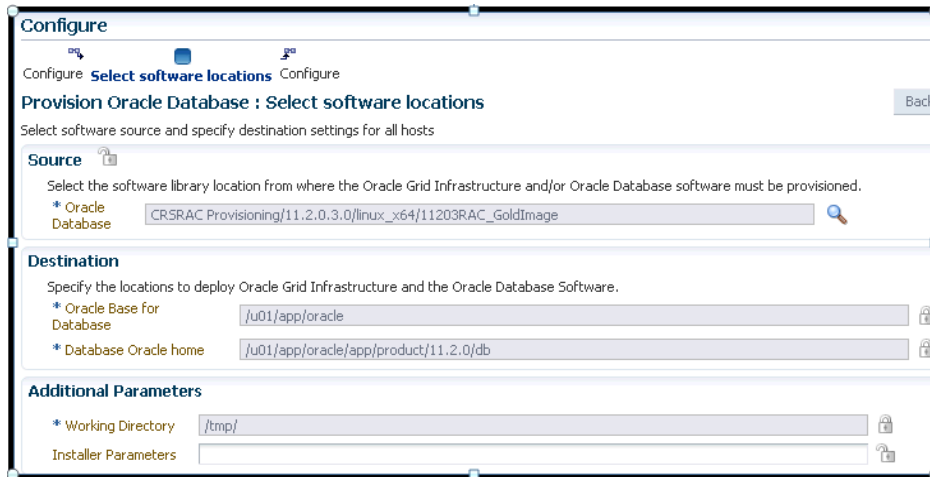
The screenshot shows the 'Select Hosts' configuration page for the 'Provision Oracle Database: prov_db_template' deployment procedure. The page has tabs for 'Select Hosts', 'Configure', 'Custom properties', 'Schedule', and 'Review'. The 'Select Hosts' tab is active. Under 'Select tasks to perform', there are sections for 'Deploy software' and 'Configure software'. The 'Deploy software' section has 'Deploy Database software' checked. The 'Configure software' section has 'Create a new database' checked. Below these is the 'Select destination hosts' section, which includes an 'Add' button and a table with columns for 'Target Name', 'Last Collection', 'Host Name', and 'Operating System'. The table is currently empty with the message 'No targets selected. To select new target(s) use 'Add...' option.'

- On the Configure page, the following configuration options appear:
 - On the Configure page, click **Setup Hosts**. Since the values here are locked by the designer, you will not be able to edit them. Click **Next** to come back to the Configure page.

This composite image shows three overlapping screenshots of the Oracle Enterprise Manager configuration pages. The top screenshot is the 'Specify OS users' page, showing options for 'Operating system users' with radio buttons for 'Use Preferred Credentials' (selected) and 'Override Preferred Credentials'. It includes a table for 'Oracle Home User' and 'Oracle Database' with dropdown menus for user types and credential sets. The middle screenshot is the 'Specify OS groups' page, showing a table for 'Operating system groups' with columns for 'Group label' and 'OS Group name'. The bottom screenshot shows a task list table with a blue circle highlighting task number 2, 'Setup hosts'.

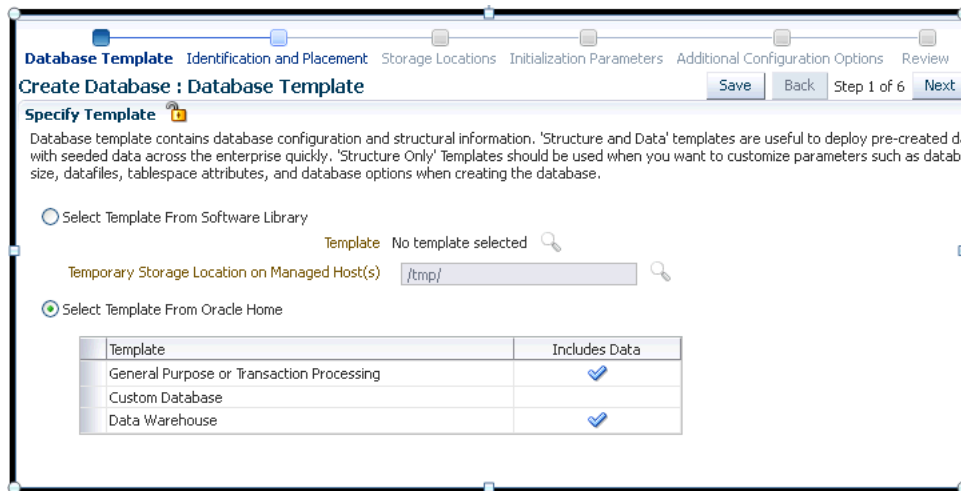
Task No.	Task	Status
1	Setup hosts	
2	Deploy software	
3	Create databases	
4	Compliance Standards	

- On the Configure page, click **Deploy Software**. Since the values here are locked by the designer, you will not be able to edit them. Click **Next** to come back to the Configure page.



- On the Configure page, click **Create Databases**. The following screen appears. Update all the fields, and click **Next** to proceed.

For information about updating the Creating Database wizard, see [Section 5.3](#).



- On the Configure page, click **Compliance Standards**. On the Configuration Standards Target Association page, select a Compliance Standard to be associated with the database. Click **Next**.



- On the Schedule page, specify a Deployment Instance name. In the Schedule section, select **Immediately**. You can set the notification preferences according to deployment procedure status, and click **Next**.

6. In the Review page, review the details you have provided for the deployment procedure and if you are satisfied with the details, then click **Finish** to run the deployment procedure according to the schedule set.

32.4.3 Step 3: Launching and Running the Saved User Defined Deployment Procedure

Log in to Enterprise Manager Cloud Control with Operator privileges to run the saved UDDP. To do so, follows these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, select **Procedure Library**.
2. On the Provisioning page, select the saved UDDP configuration template that you saved as a part of the previous step, and click **Launch**.

Note: While creating the UDDP template, if you have locked any of the values, then they will appear greyed out since they are read-only values that cannot be edited now.

3. On the Select Targets page, select the target list from the drop down menu, and click **Add** to populate the target list. Click **Next**.
4. If you declared variables that you did not define during the procedure creation, then you will have to provide the details in the Set variable page.
If you have declared a Software Library Entity variable, then you could search and select the desired entity from Software Library. Once the value is populated, you may even choose to lock this value so that any other Operator who does not have privileges on your procedure will not be able to update this values. For more information on different types of variables, see [Section 32.3.2](#). Click **Next**.
5. On the Set Credentials page, you need to set the credentials for the target host machines that you have included as a part of the `host_target_list` variable. Click **Next**.
6. On the Set Schedule and Notification page, you can schedule the job to run immediately or at a later preferred time.
7. Click **Submit**, and provide a unique **Submission Name** for your job.

32.4.4 Step 4: Tracking the Submitted User Defined Deployment Procedure

Follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, select **Procedure Activity**.
2. On the Procedure Activity page, click the job that you submitted.
3. The new Instance Execution page for the job is displayed which will give you information about the success or failure of your job for on all the targets.

For more information about the new Instance Execution page, see [Section 32.1](#).

32.5 Managing Deployment Procedures

This section contains the following:

- [Viewing, Editing, Deleting a Procedures](#)

- [Editing and Saving Permissions of a Procedures](#)
- [Tracking the Procedure Execution and Status of Deployment Procedures](#)

32.5.1 Viewing, Editing, Deleting a Procedures

To view, edit, or delete an existing procedure, follow these steps:

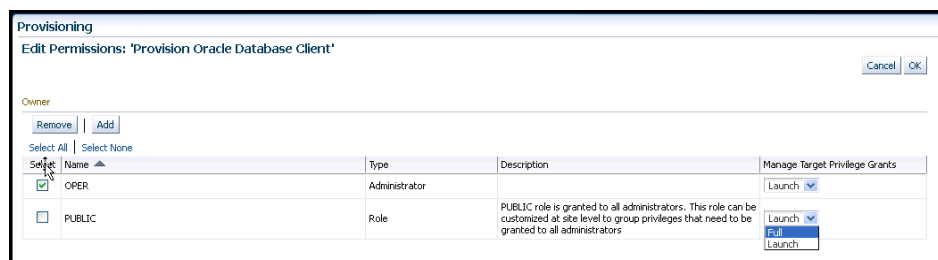
1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, do the following:
 - For Viewing the procedure, select the deployment procedure, and from the actions menu, click **View Procedure Definition**.
 - For Editing the procedure, select a user-defined procedure, and from the actions menu, select **Edit Procedure Definition** and click **Go**. If you want to customize an Oracle-provided procedure, from the actions menu, select **Create Like** and click **Go**. Save the procedure, and then customize it.
 - For Deleting the procedure, select the deployment procedure, and from the actions menu, click **Delete**.

32.5.2 Editing and Saving Permissions of a Procedures

A designer with Super Administrator privileges has the access to edit the permissions of a Deployment Procedure, and save it.

To edit the permissions on a Deployment, follow these steps:

1. In Cloud Control, from the **Enterprise** menu select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, from the actions menu select **Edit Permissions**, and then click **Go**.
3. On the Edit Permissions: <target name> page, click **Add**. From the Search and Select Administrator or Role dialog box, select the administrators or roles to which you want to grant the permissions, and click **Select**.
4. On the Edit Permissions: <target name> page, select the Role and the privileges that you want to grant to each of these roles. A *full* privilege will let the Operator edit the Deployment Procedure, and a *Launch* privilege will only allow an Operator to view and run the Deployment Procedure. Click **OK** to save these grants.



32.5.3 Tracking the Procedure Execution and Status of Deployment Procedures

After you have submitted a Deployment Procedure, you can track its status from the Procedure Completion Status page. To access this page, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, click the **Procedure Activity** tab.
3. On the Procedure Activity page, click the procedure to view the status of all deployment procedures in various stages of their lifecycle.

Table 32–4 *Deployment Procedure Status*

Status	Description
Scheduled	implies that the Deployment Procedure is scheduled to be executed at the date and time that you have specified.
Running	implies that the Deployment Procedure is currently being executed.
Action Required	Implies that the Deployment Procedure has stopped running as user interaction is required.
Suspended	Implies that the Deployment Procedure has been temporarily stopped from execution. You can resume from the paused step later.
Failed	Implies that the Deployment Procedure has failed and cannot execute the remaining steps. However, you always have the option of retrying the failed steps. Alternatively, you can ignore the error, and proceed further.
Succeeded	Implies that the Deployment Procedure has successfully completed its execution.
Skipped	Implies that the Deployment procedure has skipped the execution of this step. Primarily, a step is skipped when the condition attached to the step evaluates to false.
Stopped	Implies that the Deployment Procedure has been permanently stopped from execution by the user.
Saved	Implies that the Deployment Procedure has not been submitted for execution, and has been saved.
Completed with Errors	Indicates that the Deployment Procedure completed, but completed with errors possibly because some of the steps within it might have failed and the steps might have the <i>Skip target/Continue on Error</i> flag enabled.

You can also perform the following actions:

- a. Search for a particular Deployment Procedure using the **Search** section. Click **Search** to refine your search criteria.
- b. View the status of all Deployment Procedures. You can also manually refresh the page and view the updated status by clicking **Refresh**.
- c. View real-time status information based on a particular refresh period such as 30 seconds, 1 minute, or 5 minutes.
- d. Stop or suspend any Deployment Procedure by selecting them and clicking **Stop** or **Suspend**, respectively. You can resume at any point by clicking **Resume** or **Retry**.
- e. Delete any Deployment Procedure by selecting them and clicking **Delete**.

Note: For more information on tracking the jobs, see

32.6 Executing Procedure Instance Tasks

The following tasks can be performed from the Procedure Instance Execution page:

- [Investigating a Failed Step for a Single or a Set of Targets](#)
- [Retrying a Failed Step](#)
- [Creating an Incident](#)
- [Viewing the Execution Time of a Deployment Procedure](#)
- [Searching for a Step](#)
- [Filtering the Failed Steps](#)
- [Downloading a Step Output](#)

32.6.1 Investigating a Failed Step for a Single or a Set of Targets

Now that the design is target-centric, which means that all the targets and its corresponding steps are listed in the Procedure Steps section, you can select one target or a set of target (multiple select) from the same page to view the status of the step. To do so, perform the followings steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Activity**.
2. On the Procedure Activity page, click the procedure name to select the procedure.
3. In the Procedure Steps section, from the **View** menu, click **Expand All**.
All the steps and its corresponding status are displayed.
4. From the list select one or more targets which have a status **Fail** that you would like to investigate.
5. As you select the targets, the corresponding details are displayed on the Step Details section. You can perform one or more actions on these failed steps to proceed with the procedure execution.

32.6.2 Retrying a Failed Step

To retry a failed step, perform the following steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Activity**.
2. On the Procedure Activity page, click the procedure name to select the procedure.
3. Select the failed step from the Procedure Steps section.
The details of the step are displayed in the Setup Details section.
4. In the Setup Details section, from the **Actions** menu, click **Retry**. However, if you want to make changes to the step, select **Update and Retry** option.
5. In the Retry confirmation dialog box, click **OK** to run the step again.

32.6.3 Creating an Incident

To create an incident for the procedure execution, perform the following steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Activity**.

2. On the Procedure Activity page, click the procedure name to select the procedure.
3. In the Procedure Instance Execution page, from the **Procedure Actions** menu, select **Incident**.
4. In the incident confirmation dialog box, click **OK** to create an incident for your execution.

A confirmation dialog box appears once the incident is created. For more information about creating, packaging, and uploading an incident to an SR, see *Oracle Database Administrator's Guide*.

32.6.4 Viewing the Execution Time of a Deployment Procedure

The execution time of the deployment procedure is displayed on top of the page in the Procedure Actions section as **Elapsed Time**. The time elapsed continues to be updated until the procedure has successfully completed or has been stopped. You can resume a stopped procedure by selecting **Resume** from the **Procedure Actions** menu.

32.6.5 Searching for a Step

To search for a step that is embedded deep inside, you can use the **Expand All** option available in the **View** menu. Once the expanded list is displayed in the Procedure Step section, you can easily find the step you are looking for.

32.6.6 Filtering the Failed Steps

To view all the failed steps, perform the following:

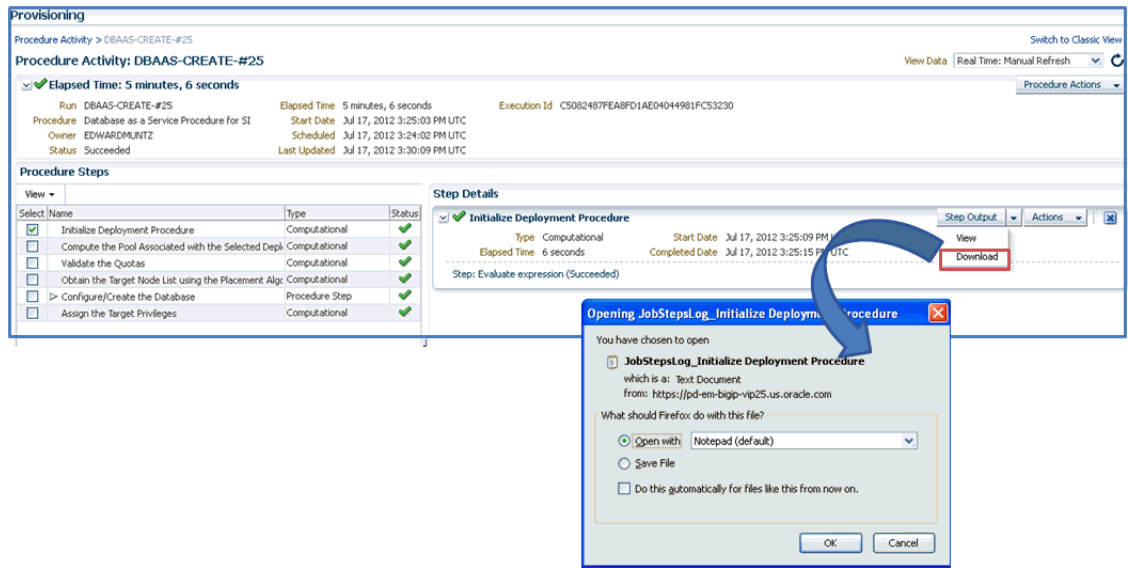
1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Activity**.
2. On the Procedure Activity page, click the procedure name to select the procedure.
3. In the Procedure Steps section, from the **View** menu, select **Filters**, and then click **Failed Status**.

All the steps that have failed are displayed in the Procedure Steps section. You can now select the steps that you want to retry, ignore, or update, and the corresponding details are displayed in the Step Details section.

32.6.7 Downloading a Step Output

To download a step output, perform the following:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Activity**.
2. On the Procedure Activity page, click the procedure name to select the procedure.
3. In the Procedure Steps section, select a step. The Step Details section displays the details of the selected step. From the **Step Output** menu, select **Download**, as shown in the following graphic to download the step output:



From the Step output menu, select **View** to view the complete output.

Customizing Deployment Procedures

The Deployment Procedures offered by Oracle Enterprise Manager Cloud Control (Cloud Control) are default procedures that have been created considering all the best practices in the industry. The steps embedded within a Deployment Procedure ensure that they meet all your provisioning and patching requirements. You can, of course, use them with the default settings to provision or patch your targets in the environment, however, you also have the choice of customizing them to include additional custom steps, disable unwanted steps, and use authentication tools to run some steps as another user.

By customizing Deployment Procedures, you can also implement different error handling methods. For example, in a patching operation where multiple hosts are patched in parallel, it may be wise to skip the host on which a failure occurs. However, failure on a device creation could render the remaining provisioning operation ineffective. Therefore, it may be necessary to abort the entire procedure for failure of such a step.

This chapter helps you understand how you can customize Deployment Procedures to make them suit your needs. In particular, this chapter covers the following:

- [Understanding Customization Types](#)
- [Customizing a Deployment Procedure](#)
- [Editing a Custom Deployment Procedure](#)
- [Changing Error Handling Modes](#)
- [Setting Up E-Mail Notifications](#)
- [Copying Customized Provisioning Entities from One Enterprise Manager Site to Another](#)
- [Customizing Directive WorkFlow Example](#)

33.1 Understanding Customization Types

The following describes the types of customization you can perform with Deployment Procedures:

Type 1

Editing Custom Deployment Procedures

You can edit an existing custom Deployment Procedure that is offered by Cloud Control to add new phases and steps. However, for patching the steps that can be added are restricted to either a Directive step or a Host command step.

You can perform the following tasks:

- Add your own phases and steps to the pre-defined blocks of the procedure structure.
- Enable and disable phases and steps
- Delete phases and steps
- Change privilege levels
- Change error handling modes
- Enable e-mail notifications

Note: You can not edit an Oracle-owned deployment procedure. To do so, you must clone the Oracle-owned procedure using Create-like functionality, and then edit the copy to include your changes.

Type 2

Creating a User Defined Deployment Procedures

You can create your own Deployment Procedure with new steps, phases, privilege levels, and so on.

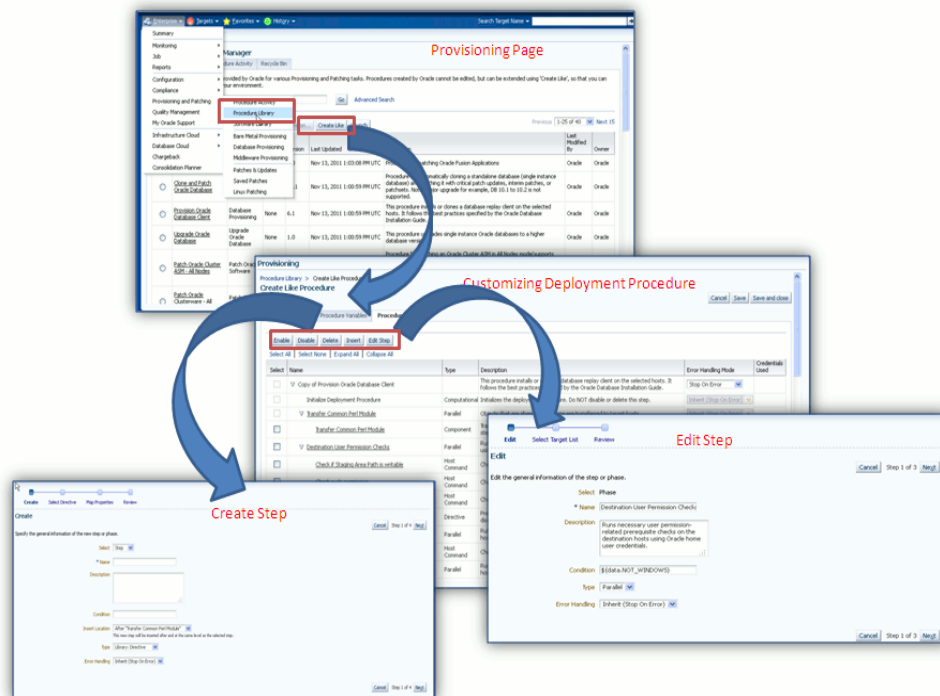
You can perform the following tasks:

- Add your own phases and steps to the pre-defined **Default phase** of the procedure structure.
- Enable and disable phases and steps
- Change privilege levels
- Change error handling modes
- Enable e-mail notifications

Note: For steps to Create a User Defined Deployment Procedure, see [Section 32.4](#).

The following graphic shows how you can use the Customizing Deployment Procedure page to create a copy of the default Deployment Procedure that is offered by Cloud Control. You can then add new steps and phases or edit the existing steps and phases in the copy to customize your procedure.

For more information on adding steps and phases, see [Section 33.2](#).



33.2 Customizing a Deployment Procedure

The first step towards customizing a Deployment Procedure is to create a copy of the default Deployment Procedure that is offered by Cloud Control. Note that only a copy can be edited and customized with your changes; the default Deployment Procedures must always and will always remain unchanged.

This section contains the following topics:

- [Adding Phases or Steps](#)
- [Adding Target Lists](#)
- [Adding Procedure Variables](#)
- [Deleting Phases or Steps](#)
- [Enabling or Disabling Phases or Steps](#)

33.2.1 Adding Phases or Steps

You can add additional phases or steps to a Deployment Procedure to run additional custom scripts, host commands, or jobs. For more information about phases and steps, see [Section 32.3.3](#).

Note: If a step is added outside a phase, then the type of step that can be added is restricted to a Job Step or a Manual Step. You can not add other steps outside a phase. However, within a phase all the steps discussed in this section can be added.

This section explains how you can add different types of phases or steps to a Deployment Procedure. In particular, it covers the following:

- [Adding Rolling or Parallel Phase](#)
- [Adding Job Step](#)
- [Adding Directive Step](#)
- [Adding Component Step](#)
- [Adding File Transfer Step](#)
- [Adding Host Command Step](#)
- [Adding Manual Step](#)

33.2.1.1 Adding Rolling or Parallel Phase

To add a rolling phase to a Deployment Procedure, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure you want to customize, and then click **Create Like**.
3. On the Create Like Procedure page, click the **Procedure Steps** tab, and then select the phase before or after which you want to add a new phase, and click **Insert**.
4. In the Create wizard, do the following:
 - a. On the Create page, specify general information about the phase as described in [Table 33-1](#).

- b. On the Select Target List page, select a target list to indicate the type of targets on which the new phase should run.

All the target lists declared while creating the procedure is listed in the drop down menu, select the target list to use for this phase. The actual targets can be chosen when the procedure is being launched.

- c. On the Review page, review the information you have provided for creating a new phase, and click **Finish**.

Table 33–1 Field Description - Adding Rolling Phase

Field Name	Description
Select	Select <i>Phase</i> .
Name	Specify a name for the custom phase.
Description	Provide a description for the custom phase.
Condition	Leave this field blank.
Insert Location	If you want to insert the custom phase after the phase or step you selected, then select After <phase or step name> . To insert it inside the phase or step selected, select Inside<phase or step> , Otherwise, select Before <phase or step> .
Type	If you are adding a rolling phase, then select <i>Rolling</i> . If you are adding a parallel phase, then select <i>Parallel</i> .
Error Handling	Select the error handling mode you want to set for the custom phase. To understand these error handling modes, see Section 33.4 .

33.2.1.2 Adding Job Step

To add a job step to a Deployment Procedure, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure you want to customize, and click **Create Like**.
3. On the Create Like Procedure page, click the **Procedure Steps** tab, and then select the step before, inside, or after which you want to add a new step, and click **Insert**.
4. In the Create wizard, do the following:

Table 33–2 Field Description - Adding Steps

Field Name	Description
Select	Select <i>Step</i> .
Name	Specify a name for the custom step.
Description	Provide a description for the custom step.
Condition	Leave this field blank.
Insert Location	If you want to insert the custom step after the step you selected, then select After <step name> . Otherwise, select Before <step> .

Table 33–2 (Cont.) Field Description - Adding Steps

Field Name	Description
Type	<ul style="list-style-type: none"> ■ For a job step, select Job. ■ For a directive step, select Library: Directive. ■ For a generic component, select Library: Component. ■ For a file transfer step, select File Transfer ■ For a manual step, select Manual. ■ For a host command step, select Host Command.
Error Handling	Select the error handling mode you want to set for the custom step. To understand these error handling modes, see Section 33.4 .

- a. On the Create page, specify general information about the step as described in [Table 33–2](#).
- b. On the Select Type page, select a job type that best describes the task that you want the step to perform. For example, if you want to job to transfer files across the network, then select **File Transfer**.
- c. On the Map Properties page, specify values for the parameters that are required by the selected job type.
- d. On the Review page, review the information you have provided for creating a new step, and click **Finish**.

33.2.1.3 Adding Directive Step

To add a directive step to a Deployment Procedure, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure you want to customize, and click **Create Like**.
3. On the Create Like Procedure page, click the **Procedure Steps** tab, and then select the step before or after which you want to add a new step, and click **Insert**.
4. In the Create wizard, do the following:
 - a. On the Create page, specify general information about the step as described in [Table 33–2](#).
 - b. On the Select Directive page, you can select one of the following options:
 - **Select New Directive:** This option lists all the directives available in Software Library, select a directive from the list that you want to run on the targets. Provide necessary values in the Select Directive section to narrow down the search results.
 - **Select New Software Library Entity Variable:** Select the Software Library variable that you declared while creating the procedure from the **Software Library Entity Variable** drop down menu. This variable behaves as a place holder and enables you the flexibility of binding it with the directives dynamically while launching the procedure. Essentially, you can use this variable to select certain entities which do not need any parameters.

For example, user-defined scripts like a perl to print the current directory location that do not need any parameters to be passed.

- Select New Software Library Entity Variable with Directive Properties:

This option allows you to bind a Software Library entity variable with a directives that are available in Software Library. Ensure that you choose a directive whose properties (signature) matches with the entity declared.

- c. On the Map Properties page, specify values for the properties associated with the selected directive. You have the option of providing or not providing the property values at this stage. If you do not provide the property values now, then they are prompted at the time of launching the procedure.
- d. On the Review page, review the information you have provided for creating a new step, and click **Finish**.

33.2.1.4 Adding Component Step

To add a generic component step to a Deployment Procedure, follow these steps:

1. In Cloud Control, from the **Enterprise** menu select **Provisioning and Patching**, and then click **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure you want to customize, and click **Create Like**.
3. On the Create Like Procedure page, click **Procedure Steps** tab, and then select the step before or after which you want to add a new step, and click **Insert**.
4. In the Create wizard, do the following:

- a. On the Create page, specify general information about the step as described in [Table 33-2](#).

- b. On the Select Component page, you can select one of the following options:

- Select New Component: This option lists all the components available in Software Library, select a component from the list that you want to run on the targets. Provide necessary values in the Select Component section to narrow down the search results.

- Select New Software Library Entity Variable: Select the Software Library variable that you declared while creating the procedure from the **Software Library Entity Variable** drop down menu. This variable behaves as a place holder and enables you the flexibility of binding it with the components dynamically while launching the procedure. Essentially, you can use this variable to select certain entities which do not need any parameters.

For example, user-defined scripts like a perl to print the current directory location that do not need any parameters to be passed.

- Select New Software Library Entity Variable with Component Properties:

This option allows you to bind the Software Library variable with the components that are available in Software Library. Ensure that you choose a component whose properties (signature) matches with the entity declared.

- c. On the Select Directive page, you can select one of the following options:

- Select New Directive: This option lists all the directives available in Software Library, select a directive from the list that you want to run on the targets. Provide necessary values in the Select Directive section to narrow down the search results.

- Select New Software Library Entity Variable: Select the Software Library variable that you declared while creating the procedure from the **Software Library Entity Variable** drop down menu. This variable behaves as a place

holder and enables you the flexibility of binding it with the directives dynamically while launching the procedure. Essentially, you can use this variable to select certain entities which do not need any parameters.

For example, user-defined scripts like a perl to print the current directory location that do not need any parameters to be passed.

- Select New Software Library Entity Variable with Directive Properties:

This option allows you to bind a Software Library entity variable with a directives that are available in Software Library. Ensure that you choose a directive whose properties (signature) matches with the entity declared.

- d. On the Map Properties page, specify values for the properties associated with the selected component and directive. You have the option of providing or not providing the property values at this stage. If you do not provide the property values now, then they are prompted at the time of launching the procedure.
- e. On the Review page, review the information you have provided for creating a new step, and click **Finish**.

33.2.1.5 Adding File Transfer Step

To add a file transfer step a Deployment Procedure, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure you want to customize, and click **Create Like**.
3. On the Create Like Procedure page, click the **Procedure Steps** tab, and then select the step before or after which you want to add a new step, and click **Insert**.
4. In the Create wizard, do the following:
 - a. On the Create page, specify general information about the step as described in [Table 33-2](#).
 - b. On the Map Properties page, select the Source Target from which you want to transfer files, the source target path, the Target Destination for file transfer and the destination path. Specify the Source and Destination Credential Usage, whether Host or Privileged Host credentials. Click **Next**.
 - c. On the Review page, review the information you have provided for creating a new step, and click **Finish**.

33.2.1.6 Adding Host Command Step

To add a host command step to a Deployment Procedure, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure you want to customize, and click **Create Like**.
3. On the Create Like Procedure page, click the **Procedure Steps** tab, and then select the step before or after which you want to add a new step, and click **Insert**.
4. In the Create wizard, do the following:
 - a. On the Create page, specify general information about the step as described in [Table 33-2](#).

- b. On the Enter Command page, specify the command or script, which you want to run on the target, and the privilege to run it.

To run the host command as a script, select **Script** from the **Command Type** list. Specify the shell that can interpret the script. The script is passed as standard input to the specified interpreter.

To run the host command as a command line, select **Single Operation** from the **Command Type** list. Specify the text you want to execute used as a command line. No assumptions are made about the shell to interpret this command line. The first entry in the command line is assumed to be the process to spawn and the rest of the command line as passed as arguments to this process. Therefore, a command line of `ls -a /tmp` spawns a process of "ls" (from the current path; also depends on the Oracle Management Agent) and passes "-a" as the first argument and then "/tmp" as the second argument to this process.

Note: The command line mode assumes that the first part of the command line is the process to be spawned. Therefore, shell internals and the commands that rely on the PATH environment variable for resolution are not recognized. If any such commands need to be used, then you need to prepend the shell that interprets the command line.

For example, the command `cd /tmp && rm -rf x` expands to "cd" as a process and then "/tmp, &&, rm, -rf, x" as arguments. To fix this, change the command line to `/bin/csh -c "cd /tmp && rm -rf x"`.

Another example, the command `export PATH=/opt:${PATH}; myopt -install` expands to "export" as a process and then "PATH=/opt:\${PATH};, myopt, -install" as arguments. To fix this, use `/bin/sh -c "export PATH=/opt:${PATH}; myopt -install"`.

- c. On the Map Properties page, specify values for the parameters that are required by the job associated with the selected component.c
- d. On the Review page, review the information you have provided for creating a new step, and click **Finish**.

33.2.1.7 Adding Manual Step

To add a manual step to a Deployment Procedure, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure you want to customize, and click **Create Like**.
3. On the Create Like Procedure page, click the **Procedure Steps** tab, and then select the step before or after which you want to add a new step, and click **Insert**.
4. In the Create wizard, do the following:
 - a. On the Create page, specify general information about the step as described in [Table 33-2](#).
 - b. On the Enter Instructions page, provide a message to inform the operator about a manual step. For example, if want to instruct the operator to log in to a system and update the kernel parameter, then specify the following:

You have been logged out of the system. Log in and update the Kernel parameters.

- c. On the Review page, review the information you have provided for creating a new step, and click **Finish**.

33.2.2 Adding Target Lists

To add one or more target lists, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure you want to customize, and click **Create Like**.
3. On the Create Like Procedure page, click **Target Lists** tab. The Default Target List `host_target_list` is displayed on the screen. To add more target lists, click **Add Row**, and enter a unique name for the Target List.

For more information about Target Lists, see [Section 32.3.1](#).

4. Click **Save**.

33.2.3 Adding Procedure Variables

To add procedure variables, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure you want to customize, and click **Create Like**.
3. On the Create Like Procedure page, click **Procedure Variables** tab.
4. Click **Add Row** to add new variables. To declare the Procedure Variable, you must enter a unique name, a description for it. Optionally, you can select the password check box to make the variable secure. You can create two types of procedure variables that can be later used while launching the deployment procedure. They are as follows: **String** and **Software Library Entity**.

For more information about Procedure Variables, see [Section 32.3.2](#).

5. Click **Save**.

Note: Procedure variables do not support default values. However, you can achieve this by saving the procedure inputs. For more information, see [Section 32.4.2](#).

33.2.4 Deleting Phases or Steps

You can delete the phases or steps that you do not want in a Deployment Procedure.

To delete phases or steps in a Deployment Procedure, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure you want to customize, and click **Create Like**.
3. On the Create Like Procedure page, click the **Procedure Steps** tab, and then select the step or phase you want to delete, and click **Delete**.

Note: Oracle recommends that you disable the steps or phases instead of deleting them because steps or phases once deleted cannot be retrieved, but steps or phases disabled can always be enabled later. For information about enabling and disabling steps or phases, see [Section 33.2.5](#).

33.2.5 Enabling or Disabling Phases or Steps

If you do not want to have some phases or steps in a Deployment Procedure, you can always disable them instead of deleting them. This is a preferred option because phases or steps once deleted cannot be retrieved, but phases or steps disabled can always be enabled later. For more information about phases and steps, see [Section 32.3.3](#).

To enable or disable phases or steps in a Deployment Procedure, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure you want to customize, and click **Create Like**.
3. On the Create Like Procedure page, do the following:
 - a. To disable a phase or step, select the phase or step you want to disable, and click **Disable**.
 - b. To enable a phase or step, select the phase or step you want to enable, and click **Enable**.

Note: For an example on enabling and disabling steps or phases, see [Section 33.3](#)

33.3 Editing a Custom Deployment Procedure

The Edit Deployment Procedure option is enabled only for Custom Deployment Procedures, which are the procedures that are not owned by Oracle. To edit an Oracle-owned procedure, you must create a copy of the procedure, and then edit the copy.

To edit an existing Custom Deployment Procedure, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select a user-defined procedure, and click **Edit Procedure Definition**.
3. In the Procedure Steps tab, insert steps or phases as explained in [Section 32.4](#). You can also Disable steps or phases by selecting the step or phase and clicking **Disable**.
4. Click **Save and Close**.

For example:

Use case: Customizing Oracle RAC Deployment Procedure to use as Oracle Grid Infrastructure Deployment Procedure (Example Use Case)

In Enterprise Manager 12c, there is no option for provisioning only the Oracle Grid Infrastructure. To do so, you must choose **Provision Oracle RAC Database**, and then disable all the Oracle RAC specific steps from the deployment procedure, and save it as a new custom procedure. This new procedure when run provisions only Oracle Grid Infrastructure on the selected targets.

To achieve this, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. On the Database Provisioning page, select **Provision Oracle RAC Database**, and click **Create Like**.
3. On the Create Like Procedure page, change the name of the Deployment Procedure to **Provision Oracle Grid Infrastructure**, and then click **Save and close**.
4. On the Provisioning page, select the **Provision Oracle Grid Infrastructure** procedure, and click **Edit Procedure Definition**.
5. In the Procedure Steps tab, search for the step **Prepare Database Stage Area**. Disable the selected step, and all the following steps, and then click **Save and Close**.
6. Select the custom copy of **Provision Oracle RAC Database**, and click **Launch**. Fill all the necessary details, and submit this procedure to provision only Oracle Grid Infrastructure on the selected targets.

33.4 Changing Error Handling Modes

Every step in a Deployment Procedure is preconfigured with an error handling mode that indicates how the Deployment Procedure will behave when the phase or step encounters an error. The error handling modes offered by Cloud Control are:

- *Inherit* - Inherits the error handling mode that was set for the enclosing phase. (When set for a step that is outside a phase, it inherits the error handling mode from the Deployment Procedure).
- *Stop On Error* - Stops when an error is encountered. Deployment Procedure does not proceed to the next step until you correct the errors or override them.
- *Continue On Error* - Continues even when an error is encountered.
- *Skip Target* - Ignores the failed target on the list and continues with other targets.

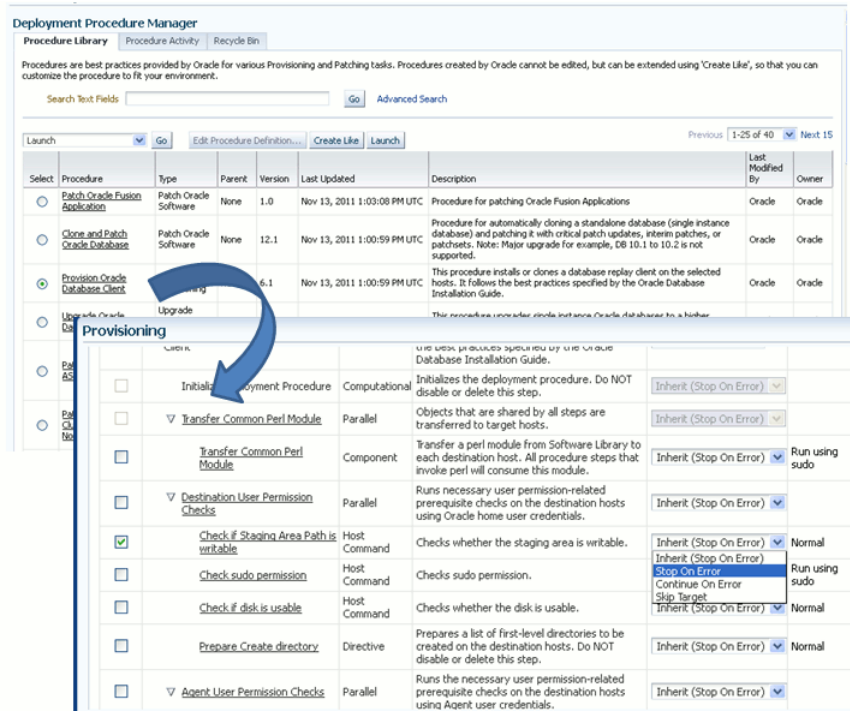
For more information about steps, see [Section 32.3.3](#).

To change the error handling modes, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure you want to customize, and click **Create Like**.
3. On the Create Like Procedure page, click the **Procedure Steps** tab, and then select a phase or step, and change the **Error Handling Mode**.

Once the mode is selected from the list, Cloud Control automatically refreshes the page with the newly selected mode for that phase or step.

The following is an example that illustrates how you customize the *Oracle Database Provisioning* Deployment Procedure to change the error handling mode of the *Destination User Permission Checks* phase:



33.5 Setting Up E-Mail Notifications

Cloud Control can send e-mail notifications to report the status of a Deployment Procedure. However, by default, Deployment Procedures do not have this feature enabled. For e-mail notifications to be sent, your Super Administrator must configure an Outgoing Mail (SMTP) Server within Enterprise Manager, and then you as an Administrator must provide your E-mail Address and Password for receiving notifications.

Enabling E-mail notifications is a two-step process:

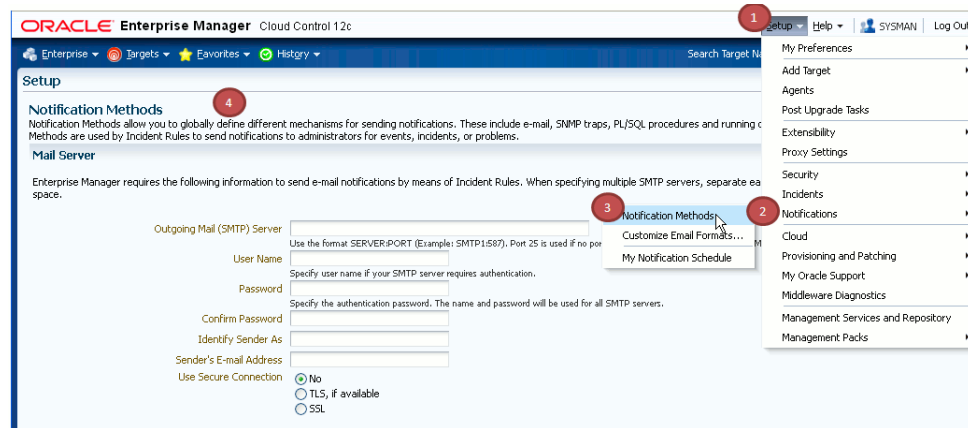
- [Configuring an Outgoing Mail \(SMTP\) Server Within Enterprise Manager](#)
- [Providing the Administrator Enterprise Manager E-mail and Password](#)

IMPORTANT: As a prerequisite, you are expected to have configured the Mail Server and set up the e-mail address in Cloud Control.

33.5.1 Configuring an Outgoing Mail (SMTP) Server Within Enterprise Manager

Before Enterprise Manager can send e-mail notifications, you must first set up the Outgoing Mail (SMTP) servers.

Note: Only a privileged user can configure SMTP servers.



To set up the SMTP server, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Notification**, then select **Notifications Method**.
2. On the Setup page, in the Mail Server section, enter one or more outgoing mail servers and optional port number (if left blank, port 25 is used by default).
3. Enter the mail server authentication credentials like **UserName**, **Password**. The UserName and Password fields allow you to specify a single set of authentication credentials to be used for all mail servers. If no mail server authentication is required, leave the User Name, Password (and Confirm Password) fields blank.
4. Enter the name you want to appear as in the sender of the notification messages field **Identify Sender As**.
5. Enter the e-mail address you want to use to send your e-mail notifications in the **Sender's E-mail Address**. When using incident rules, any e-mail delivery problems will be automatically sent to the **Sender's E-mail Address**.

Note: The e-mail address you specify on this page is not the e-mail address to which the notification is sent. You will have to specify the e-mail address (where notifications will be sent) from the Preferences General page. For information on specifying e-mail addresses for e-mail notification, see [Section 33.5.2](#)

6. The Use Secure Connection option allows you to choose the SMTP encryption method to be used. Three options are provided:
 - **No:** E-mail is not encrypted.
 - **SSL:** E-mail is encrypted using the Secure Sockets Layer protocol.
 - **TLS, if available:** E-mail is encrypted using the Transport Layer Security protocol if the mail server supports TLS. If the server does not support TLS, the e-mail is automatically sent as plain text.

For example,

In the following example, two mail servers are specified--smtp01.example.com on port 587 and smtp02.example.com on port 25 (default port). A single administrator account (myadmin) is used for both servers.

Outgoing Mail (SMTP) Server smtp01.example.com:587, smtp02.example.com

User Name myadmin

Password *****

Confirm Password *****

Identify Sender As EMD Notifications

Sender's E-mail Address mgmt_rep@example.com

Use Secure Connection: SSL

33.5.2 Providing the Administrator Enterprise Manager E-mail and Password

You specify one or more e-mail addresses to which notifications can be sent when you define the Notifications Schedule. In addition to defining notification e-mail addresses, you associate the notification message format (long or short) to be used for each e-mail address.

Each e-mail address can have up to 128 characters; there is no upper bound with the number of e-mail addresses.

To add an e-mail address:

1. In Cloud Control, from the **Setup** menu, select **Notification**, then select **My Notifications Schedule**.
2. Specify an Enterprise Manager administrator, and click **Define Schedule**.
3. If no previous e-mail addresses have been defined for the administrator, a message displays prompting your to define e-mail addresses for the administrator. Click **Click here to set e-mail addresses**. The General page appears.
4. Click **Add Another Row** to create a new e-mail entry field in the E-mail Addresses table.
5. Specify the e-mail address associated with your Enterprise Manager account. All e-mail notifications you receive from Enterprise Manager will be sent to the e-mail addresses you specify. For example, user1@example.com, user2@example.com, and so on.
6. If you need to additional e-mail addresses, click **Add Another Row**, enter the e-mail address and select the format.
7. You can test if the e-mail address is properly configured to receive e-mails from Enterprise Manager by selecting it and clicking **Test**.
8. Click **Apply** to save your changes when finished.

Once you have defined your e-mail notification addresses, they will be shown when you define a notification schedule. For example, user1@example.com, user2@example.com, user3@example.com. You can choose to use one or more of these e-mail addresses to which e-mail notifications for the Incident Rule will be sent.

33.6 Copying Customized Provisioning Entities from One Enterprise Manager Site to Another

If you have customized provisioning entities on an Enterprise Manager installation that you want to apply to another installation of Enterprise Manager, follow these steps. The provisioning entities can include procedure definitions or Software Library entities or a combination of these.

Prerequisites

Ensure that:

- Customized provisioning entities exist in the system at source site.
- Source administrator has access to the customized provisioning entities at source site.
- Source administrator has necessary privileges to export the provisioning entities.
- Destination site has similar setup as source site, that is, both have the same version of Enterprise Manager installed.
- Destination administrator has privileges to import provisioning entities.

Copying Customized Provisioning Entities

Follow these steps:

1. Export the PAR file using the following command:

```
emctl partool export -guid <procedure guid> -file <file> -displayName <name>
-description <desc> -metadataOnly(optional)
```

2. For importing the provisioning entities, you can use `emctl partool` as follows:

```
emctl partool <deploy|view> -parFile <file> -force(optional)
emctl partool <deploy|view> -parFile <file> -force(optional) -ssPasswd
<password>
emctl partool <deploy|view> -parDir <dir> -force(optional)
```

3. Alternatively, you can import the PAR file from Cloud Control as explained in the following steps.
 - a. From the **Enterprise** menu, select **Provisioning and Patching** and then select **Procedure Library**.
 - b. On the Procedure Library page, from the list, select **Import** and click **Go**.
4. In the Upload Procedure File page, select:
 - Upload From Local Machine, if the PAR files are stored on your local machine. Click **Browse** and select the PAR File to Upload. Click **Import**.
 - Upload From Management Agent Machine, if you have stored the PAR files on the Management Agent machine. Click **Target** and select the Host. Click **Select File** and select the PAR file. Click **Import**.
5. Apply the imported entities.

33.7 Customizing Directive WorkFlow Example

Directives are essentially scripts stored in the Software Library. They are used in Deployment Procedures within a Directive Step, which is a special type of action step. For more information about Directive Step, see [Section 32.3.3](#).

If you want to customize a directive offered by Cloud Control, then first create a copy of the Perl script associated with that Directive and make a new directive out of that copy. Then customize the Deployment Procedure to modify a step to use this new directive, and then schedule the deployment. This section explains the following:

- [Creating and Uploading Copy of a Default Directive](#)
- [Customizing Deployment Procedure to Use the New Directive](#)

- [Running the Customized Deployment Procedure](#)

33.7.1 Creating and Uploading Copy of a Default Directive

To create a new customized directive using a default directive, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library page, from the table, expand the Software Library and the other levels under this category to reach the directive you want to copy.

For example, if you want to copy the Apply Patch directive of a patching operation, then expand **Software Library** and then expand **Patching**. From this level, expand **Common**, and then **All**, and finally **Generic**. Under Generic, you should see the directive **Apply Patch**.

3. Select the directive you want to copy and click **Create Like**, and store the copy of the directive in a custom folder called **Directive**.
4. Select the custom directive, and then click **Edit**.
5. In the Create Directive wizard, do the following:
 - a. On the Describe page, describe the directive you are creating.
 - b. On the Configure page, click **Add** to specify the command line arguments to be passed to the Directive. Set the **Shell Type** to Perl because you are adding a Perl script. If the script is neither Perl nor Bash, then set it to **Defined in Script**.

Each entry represents a single command line argument. Each argument may include a variable to be set later, a prefix and suffix. The prefix and suffix text are appended before and after the property value to produce the command line argument.

Repeat this step to add all the command line arguments.

- c. On the Select Files page, select **Upload Files**. In the Specify Source section, select **Local Machine**, and click **Add** to select the modified perl file.
- d. Click **Save and Upload**.

33.7.2 Customizing Deployment Procedure to Use the New Directive

To customize a Deployment Procedure to use the new directive, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the Deployment Procedure for which you want to use this new directive, and click **Create Like**.
3. On the Create Like Procedure page, select **Procedure Steps** tab, and do the following:
 - a. From the table that lists all the steps within that Deployment Procedure, select the directive step with which you want to associate the new directive, and click **Edit Step**.
 - b. In the Edit Directive Step wizard, do the following:
 - a. On the Edit page, click **Next**.

- b. On the Select Directive page, select **Select New Directive**. Then search and select the new directive you created, and click **Next**.
 - c. On the Map Properties page, specify the values for the directive properties, and click **Next**.
 - d. On the Review page, click **Finish**.
- c. Click **Save**.

33.7.3 Running the Customized Deployment Procedure

To run the customized Deployment Procedure, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, select the customized Deployment Procedure and click **Schedule Deployment**.

Part XI

Additional Information

This part contains the following appendixes:

- [Appendix A, "Using Enterprise Manager Command Line Interface"](#)
- [Appendix B, "Checking Host Readiness"](#)
- [Appendix C, "Using emctl partool Utility"](#)
- [Appendix D, "Understanding PXE Booting and Kickstart Technology"](#)
- [Appendix E, "Troubleshooting Issues"](#)
- [Appendix F, "Oracle Site Guard Command-Line Interface Reference"](#)

Using Enterprise Manager Command Line Interface

This chapter explains how to use Enterprise Manager Command Line Interface (EM CLI) to deploy patches using Patch Plans, provision procedures, and perform some of the Software Library tasks.

In particular, this chapter covers the following:

- [Overview](#)
- [Prerequisites](#)
- [Enterprise Manager Command Line Interface Verbs](#)
- [Provisioning Using EM CLI](#)
- [Patching Using EM CLI](#)
- [WorkFlow Examples Using EM CLI Commands](#)
- [Limitations of Using Enterprise Manager Command Line Interface](#)

Note: The entire EM CLI implementation for running the various Deployment Procedures has been revamped in Oracle Enterprise Manager Cloud Control (Cloud Control).

A.1 Overview

Enterprise Manager Command Line Interface (EM CLI) is a command line utility available for power users in Oracle Enterprise Manager Cloud Control (Cloud Control) that enables you to perform most of the console-based operations. It enables you to access Cloud Control functionality from text-based consoles (shells and command windows) for a variety of operating systems.

Using EM CLI you can:

- Perform various command line operations such as monitoring and managing targets, jobs, running deployment procedures, patching Enterprise Manager targets, and so on.
- Use the functions available with EM CLI called *verbs*, to build your custom scripts on various programming environments like Operating System shell, Perl, Python, and so on. This in turn allows you to closely integrate Oracle Enterprise Manager functionality with your own enterprise business process.
- Carry out operations with the same security and confidentiality as the Cloud Control console.

A.2 Prerequisites

Before using EM CLI, ensure that you meet the following requirements:

- EM CLI client must be set up. To do so, see *Oracle Enterprise Manager Command Line Interface*.
- Targets that will be supplied to the Deployment Procedures should be managed by Enterprise Management 12c Management Agents.
- If you are patching in the offline mode, with no internet connectivity, then ensure that the patches are available in the Software Library before running the EM CLI commands.

A.3 Enterprise Manager Command Line Interface Verbs

This section primarily lists all the EM CLI verbs used for accomplishing the various patching and provisioning tasks. Primarily, it contains:

- [Provisioning EM CLI Verbs](#)
- [Patching EM CLI Verbs](#)
- [Software Library EM CLI Verbs](#)

Note: For information about Enterprise Manager 12c verb usage, syntax, and examples, see *Oracle Enterprise Manager Command Line Interface*

A.3.1 Provisioning EM CLI Verbs

This section describes the usage of EM CLI verbs to run Deployment Procedures in Enterprise Manager 12c:

- [New Enterprise Manager Command Line Interface Verbs](#)
- [Obsolete Enterprise Manager Command Line Interface Verbs](#)
- [Enterprise Manager Command Line Interface Verbs for Running Procedures](#)

A.3.1.1 New Enterprise Manager Command Line Interface Verbs

The new EM CLI verbs introduced in Cloud Control are:

- `describe_procedure_input`
- `save_procedure_input`
- `update_procedure_input`
- `get_executions`
- `get_instance_data` (replaces `get_instance_data_xml`)

The EM CLI verb that has been modified to support additional arguments in Enterprise Manager 12c is `submit_procedure`. The following table compares the old and the current arguments supported by the `submit_procedure` verb:

submit_procedure arguments (as in EM 11g)	submit_procedure arguments (as in EM 12c)
<pre>emcli submit_procedure -procedure='guid of the procedure' -input_file="data:file_path" [-instance_name="name of the procedure instance"] [-schedule=start_time:yyyy/MM/dd HH:mm;tz:{java timezone ID}]</pre>	<pre>emcli submit_procedure [-name={name of the procedure}] [-owner={owner of the procedure}] [-procedure={guid of the procedure}] -input_file={data:{file_path}/file name} [-instance_name={name of the procedure instance}] [-notifications={procedure status}] [-grants={users and their corresponding accessing levels}] [-schedule=start_time:yyyy/MM/dd HH:mm;tz:{java timezone ID}]</pre>
<p>Submitting the procedure was possible only using the procedure GUID</p>	<p>Note: All the new arguments have been highlighted in bold font.</p> <p>Starting with Enterprise Manager 12c, procedure can be submitted either using the procedure GUID or using the procedure name /owner pair.</p>

A.3.1.2 Obsolete Enterprise Manager Command Line Interface Verbs

The following EM CLI verbs are included for backward compatibility, however they are deprecated and Oracle recommends you move to the new commands:

- get_instance_data_xml
- set_instance_jobgrants

Note: For information about the Enterprise Manager 11g verbs, see *Enterprise Manager Command Line Interface* available in the following doc library:

<http://www.oracle.com/pls/em111/docindex>

A.3.1.3 Enterprise Manager Command Line Interface Verbs for Running Procedures

Here is a list of all the EM CLI verbs used for running deployment procedures:

Table A-1 EM CLI Provisioning Verbs and their Usage

Verb	Usage	Example
confirm_instance	<pre>emcli confirm_instance [-instance={instance guid}] [-exec={execution guid}] -stateguid={state guid}</pre>	<pre>emcli confirm_instance -instance=234RTGHJ096YHN5KM 2IKJM567 -stateguid=56IUJMN029IJ3ERF G09IKJ</pre>

Table A-1 (Cont.) EM CLI Provisioning Verbs and their Usage

Verb	Usage	Example
describe_ procedure_input	emcli describe_procedure_input [-procedure={procedure GUID}] [-name={procedure name or procedure configuration}] [-owner={owner of the procedure or procedure configuration}] [-parent_ proc={procedure of the procedure configuration. this only applies to describe a procedure configuration with the same name}]	emcli get_procedure_xml -procedure=16B15CB29C3F9E6C E040578C96093F61 > proc.properties
delete_instance	emcli delete_instance [-instance={instance guid}] [-exec={execution guid}]	emcli delete_instance -instance=234RTGHJ096YHN5KM 2IKJM567
get_executions	emcli get_executions -instance={instance GUID}	emcli get_executions -instance=16B15CB29C3F9E6CE 040578C96093F61
get_instances	emcli get_instances [-type={procedure type}]	emcli get_instances -type=DemoNG
get_instance_data	emcli get_instance_data [-instance={instance guid}] [-exec=execution guid]	emcli get_instance_data -instance=16B15CB29C3F9E6CE 040578C96093F61 > instanceData.properties
get_instance_ status	emcli get_instance_status [-instance={instance guid}] [-exec=execution guid] [-xml [-details] [-showJobOutput] [-tailLength={last N characters}]]]	emcli get_instance_status -instance=1TYUIOPLKMUHKJANG S09OIJ -xml -details -showJobOutput
get_retry_argument	emcli get_retry_arguments [-instance={instance guid}] [-exec=execution guid] [-stateguid={state guid}]	emcli get_retry_argument -instance=16B15CB29C3F9E6CE 040578C96093F61 -stateguid=4IUOHNAG29KLNLOK JGA
get_procedures	emcli get_procedures [-type={procedure type}] [-parent_proc={procedure associate with procedure configuration}]	emcli get_procedures -type=DemoNG -parent_ proc=ComputeStepTest
get_procedure_xml	emcli get_procedure_xml [-procedure={procedure guid}] [-name={procedure name}] [-owner={procedure owner}]	emcli get_procedure_xml -procedure=16B15CB29C3F9E6C E040578C96093F61 > proc.xml
get_procedure_ types	emcli get_procedure_types	emcli get_procedure_types
ignore_instance	emcli ignore_instance [-instance={instance guid}] [-exec=execution guid] [-stateguid={state guid}]	emcli get_retry_argument -instance=16B15CB29C3F9E6CE 040578C96093F61 -stateguid=4IUOHNAG29KLNLOK JGA, 29C3F9E6CE040578C96093F 61KNALK

Table A-1 (Cont.) EM CLI Provisioning Verbs and their Usage

Verb	Usage	Example
reschedule_instance	emcli reschedule_instance [-instance={instance guid}] [-exec=execution guid] -schedule=start_time:yyyy/MM/dd HH:mm;tz:{java timezone id};	emcli reschedule_instance -instance=1TYUIOPLKMUHKJANG S090IJ -schedule="start_ time:2012/12/25 00:00;tz:American/New York;grace_period:60"
resume_instance	emcli resume_instance [-instance={instance guid}] [-exec=execution guid]	emcli resume_instance -instance=1TYUIOPLKMUHKJANG S090IJ
save_procedure	emcli save_procedure_input -name={name of procedure configuration} -procedure={Procedure name} [-owner={owner of procedure}] -input_file=data:/file path/file name [-grants={users and their corresponding accessing levels}] [-notification={procedure status}] [-schedule=start_ time:yyyy/MM/dd HH:mm;tz:{java timezone id};grace_period:xxx]	emcli save_procedure_input -name=procConfiguration -procedure=ComputeStepTest -input_ file=data:/home/data.proper ties -grants="user1:VIEW_ JOB; user2:FULL_JOB" -notification="sheduled, action required, running" -schedule="start_ time:2012/12/25 00:00;tz:American/New York;grace_period:60"
stop_instance	emcli stop_instance [-instance={instance guid}] [-exec=execution guid]	emcli stop_instance -instance=1TYUIOPLKMUHKJANG S090IJ
submit_procedure	emcli submit_procedure [-name={name of the procedure}] [-owner={owner of the procedure}] [-procedure={guid of the procedure}] -input_ file={data:{file_path}/file name" [-instance_name={name for the procedure instance}] [-notification={procedure status}] [-grants={users and their corresponding accessing levels}] [-schedule=start_time:yyyy/MM/dd HH:mm; tz:{java timezone ID}]	emcli submit_procedure -input_file=data:data.xml -procedure=16B15CB29C3F9E6C E040578C96093F61 -schedule="start_ time:2006/6/21 21:23; tz:America/New_York" -grants="user1:VIEW_JOB; user2:FULL_JOB" -notification="sheduled, action required, running"
suspend_instance	emcli stop_instance [-instance={instance guid}] [-exec=execution guid]	emcli suspend_instance -instance=1TYUIOPLKMUHKJANG S090IJ
update_and_retry_step	emcli update_and_retry_step [-instance={instance guid}] [-exec=execution guid] [-stateguid={stateguid1, stateguid2, ...}] [-args="command1:value1;command2: value2;...]	emcli get_retry_argument -instance=16B15CB29C3F9E6CE 040578C96093F61 -stateguid="4IUOHNAG29KLNLO KJGA,PO82NLKBSAKBNIUPOQTG" -args="command1:a; command2:b"

Table A-1 (Cont.) EM CLI Provisioning Verbs and their Usage

Verb	Usage	Example
update_procedure_input	emcli update_procedure_input -name={name of procedure configuration} -input_file="data:/file path/file name" [-notification={procedure status}][-grants={users and their corresponding accessing levels}] [-schedule=start_time:yyyy/MM/dd HH:mm;tz:{java timezone id};grace_period:xxx]	emcli update_procedure_input -name=procConfiguration -input_file=data:/home/data.properties -grants="user1:VIEW_JOB;user2:FULL_JOB" -notification="sheduled, action required, running" -schedule="start_time:2012/12/25 00:00;tz:American/New York;grace_period:60"

A.3.2 Patching EM CLI Verbs

Support for patching any number of targets from the same single patch plan using command line interface is now supported. Following are some of the important EM CLI verbs used for patching.

Table A-2 EM CLI Patching Verbs and their Usage

Verbs	Usage	Example
create_patch_plan	emcli create_patch_plan -name="name" -input_file=data:"file_path" [-impact_other_targets="add_all add_original_only cancel"][-problems_assoc_patches="ignore_all_warnings cancel"]	emcli create_patch_plan -name="plan name" -input_file=data:"/tmp/patchplan.pros" -impact_other_targets="add_all"
describe_patch_plan_input	emcli describe_patch_plan_input -name="name"	emcli describe_patch_plan_input -name="plan_name"
get_patch_plan_data	emcli get_patch_plan_data -name="name"	emcli get_patch_plan_data -name="plan_name"
set_patch_plan_data	emcli set_patch_plan_data -name="name" [-impact_other_targets=" add_all add_original_only cancel"][-problems_assoc_patches=" ignore_all_warnings cancel"]	emcli set_patch_plan_data -name="plan name" -input_file=data:"/tmp/patchplan.pros" -impact_other_targets="add_all"
list_aru_languages	emcli list_aru_languages [-name="language name" -id="language id"] [-noheader] [-script -format=[name:<pretty script csv>; [column_separator:"column_sep_string"]; [row_separator:"row_sep_string"];]	emcli list_aru_languages -noheader
list_aru_platforms	emcli list_aru_platforms [-name="platform name" -id="platform id"] [-noheader] [-script -format=[name:<pretty script csv>; [column_separator:"column_sep_string"]; [row_separator:"row_sep_string"];]	emcli list_aru_platforms -noheader

Table A-2 (Cont.) EM CLI Patching Verbs and their Usage

Verbs	Usage	Example
list_aru_products	emcli list_aru_products [-name="product name" -id="product id"] [-noheader] [-script -format= [name:<pretty script csv>; [column_separator:"column_sep_ string"]; [row_separator:"row_ sep_string"];]	emcli list_aru_products -id="product id"
list_aru_releases	emcli list_aru_releases [-name="release name" -id="release id" -productId="product id"] [-noheader] [-script -format= [name:<pretty script csv>; [column_separator:"column_sep_ string"]; [row_separator:"row_ sep_string"];]	emcli list_aru_releases -noheader
list_patch_plans	emcli list_patch_plans -name="name" [-noheader] [-script -format= [name:<pretty script csv>; [column_separator:"column_sep_ string"]; [row_separator:"row_ sep_string"];]	emcli list_patch_plans -name="plan name" -noheader
search_patches	emcli search_patches [-swlib] [-patch_name="patch_name"] [-product="product id" [-include_ all_products_in_family]] [-release="release id"] [-platform="platform id" -language="language id"] [-type="patch patchset"] [-noheader] [-script -xml -format= [name:<pretty script csv>; [column_separator:"column_sep_ string"]; [row_separator:"row_ sep_string"];]	emcli search_patches -patch_name="patch number" -platform="platform id"
get_connection_mode	emcli get_connection_mode	emcli get_connection_mode
set_connection_mode	emcli set_connection_mode -mode="online offline"	emcli set_connection_mode -mode="offline"
show_patch_plan	emcli show_patch_plan -name="name" [-info [-showPrivs]] [-actions [-onlyShowEnabled]] [-patches] [-targets] [-deplOptions] [-analysisResults] [-conflictFree] [-impactedTargets] [-deploymentPro cedures]	emcli show_patch_plan -name="plan name" -info -showPrivs
submit_patch_plan	emcli submit_patch_plan -name="name" -action="action name"	emcli submit_patch_plan -name="plan name" -action="analyze"

Table A-2 (Cont.) EM CLI Patching Verbs and their Usage

Verbs	Usage	Example
get_targets	emcli get_targets [-targets="[name1:]type1;[name2:] type2;..."] [-alerts] [-noheader] [-script -format=[name:<pretty script csv>]; [column_separator:"column_sep_ string"]; [row_separator:"row_sep_ string"];]	emcli get_targets -targets="databa%:%oracle%"
get_instance_ status	emcli get_instance_status [-instance={instance_guid}] [-exec={execution_guid}] [-name={execution name}] [-owner={execution owner}] [-xml [-details]	emcli get_instance_status -instance=16B15CB29C3F9E6CE 040578C96093F61 -xml -showJobOutput -tailLength=1024
get_job_ execution_detail	emcli get_job_execution_detail -execution={execution_id} [-xml [-showOutput [-tailLength={length}]]]	emcli get_job_execution_ detail -execution=1234567890123456 7890123456789012 -xml
create_named_ credential	emcli create_named_credential -cred_name=<name> -auth_target_ type=<authenticating target type> -cred_type=<Credential type> -cred_scope=<Credential Scope> -cred_desc=<Credential Description> -target_ name=<target name> -target_ type=<target type> -input_ file=<tag:value> -input_ bfile=<tag:value> -properties_ file=<filename> -attributes=<p1:v1;p2:v2;...>	emcli create_named_ credential -cred_name=NC1 -auth_target_ type=host-cred_ type=HostCreds -attributes="HostUserName:f oo;HostPassword:"
get_named_ credential	emcli get_named_credential -cred_owner=<owner> -cred_ name=<name> -out=<filename>	emcli get_named_credential -cred_name=NC1
set_preferred_ credential	emcli set_preferred_credential -set_name="set_name" -target_ name="target_name" -target_ type="ttype" -credential_ name="cred_name" [-credential_ owner="owner"]	emcli set_preferred_ credential -target_ type=oracle_database -target_name=myDB -set_ name=DBCredsSYSDBA -credential_ name=MyDBCredentials -credential_owner="Joe"
show_credential_ set_info	emcli show_credential_type_info [-target_type="target_type"] [-type_name="credential_type_ name"]	emcli show_credential_type_ info -target_type=oracle_ database
setup	emcli setup - url="http[s]://host:port/em/" [-username=<EM Console Username>] [-password=<EM Console Password>] [-licans=YES NO] [-dir=< local emcli configuration directory>] [-trustall] [-novalidat e] [-noautologin] [-custom_attrib file=<Custom attribute file path>] [-nocertvalidate]	emcli setup -url=https://dadvmi0128.us. example.com:4473/em -username=sysman -password=sysman

Table A–2 (Cont.) EM CLI Patching Verbs and their Usage

Verbs	Usage	Example
upload_patches	emcli upload_patches -from_ host="host name" -patch_ files="metadata file path;ZIP file path" [-cred_name="name" -cred_owner="owner"]	emcli upload_patches -patch_ files="/scratch/p13741363_ 112310_Linux-x86-64_ M.xml;/scratch/p13741363_ 112310_Linux-x86-64.zip" -from_host=h1.us.oracle.com
delete_patches	emcli delete_patches -patch_ name="patch name" -release="release id" -platform= "platform id"	emcli delete_patches -patch_name=13741363 -release=80112310 -platform=226

A.3.3 Software Library EM CLI Verbs

Support for configuring Software Library, creating entities, and using them has been introduced in Oracle Enterprise Manager Cloud Control 12c Release 2 (12.1.0.2).

Note: You can either use Enterprise Manager UI or the command line utility (EM CLI) to retrieve the folder id and the entity revision id. To do so, and for a comprehensive example on how to effectively use the EM CLI verbs to perform a number of Software Library tasks listed in the following table, see the workflow example [Section A.6.5](#).

Following are some of the important EM CLI verbs used to perform some Software Library actions:

Table A–3 Software Library EM CLI Verbs and Their Usage

Verb	Usage	Example
add_swlib_storage_ location (Adding a Software Library storage location)	emcli add_swlib_storage_ location -name="location_ name" -path="location_path" [-type="OmsShared OmsAgent Ht tp Nfs ExtAgent"] [-host="hostname"] [-credential_set_ name="setname"] [-credential_name="name" -credential_owner="owner"]	emcli add_swlib_storage_ location -name="myOMSAGtLocation" -path="/u01/swlib" -type="OmsAgent" -host="fs1.us .example.com" -credential_ name="MyexampleCreds" -credential_owner="example_ USER"
create_swlib_folder (Creating a Software Library folder)	emcli create_swlib_folder -name="folder_name" -parent_ id="parent folder id" [-desc="folder description"]	emcli create_swlib_folder -name="myFolder" -parent_ id="oracle:defaultService:em: provisioning:1:cat:B13B3B7B08 6458CFE040E80A19AA560C" -desc="myFolder description"

Table A-3 (Cont.) Software Library EM CLI Verbs and Their Usage

Verb	Usage	Example
create_swlib_entity (Creating a Software Library entity)	emcli create_swlib_entity -name="entity_name" -folder_ id="folder_id" [-type]="type internal id"] [-subtype]="subtype internal id"] [-desc="entity_desc"] [-attr="<attr name>:<attr value>"] [-prop="<prop name>:<prop value>"] [-secret_prop="<secret prop name>:<secret prop value>"] [-note="note text"]	emcli create_swlib_entity -name="myexampleInstall" -folder_ id="oracle:defaultService:em: provisioning:1:cat:B13B3B7B08 6458CFE040E80A19AA560C" -desc="myexampleInstall description" -attr="PRODUCT:example" -attr="PRODUCT_VERSION:3.0" -attr="VENDOR:example Corp" -prop="DEFAULT_ HOME:/u01/example3/" -note="myexampleInstall for test servers"
list_swlib_entities (Listing the Software Library entities)	emcli list_swlib_entities [-name="entity_name"] [-folder_id="folder internal id"] [-desc="entity_desc"] [-attr="<attr name>:<attr value>"] [-type]="type internal id"] [-subtype]="subtype internal id"] [-maturity]="maturity"] [- owner]="owner"] [-status]="sta tus"] [-show_folder_path] [-show_folder_id] [-show_ entity_rev_id]	emcli list_swlib_entities -name="myEntity" -attr="PRODUCT=Oracle Database" -show_folder_id
list_swlib_entity_ subtypes (Listing Software Library entity subtypes)	emcli list_swlib_entity_ subtypes -entity_type_ id="type internal name"] [-show_subtype_id]	emcli list_swlib_entity_ subtypes -entity_type_ id="COMP_Component" -show_ type_id
list_swlib_entity_ types (Listing Software Library entity types)	emcli list_swlib_entity_types [-show_type_id]	emcli list_swlib_entity_types -show_type_id
list_swlib_folders (Listing Software Library folders)	emcli list_swlib_ folders [-parent_id="parent folder id"] [-show_folder_ path] [-show_folder_id]	emcli list_swlib_folders -parent_ id="oracle:defaultService:em: provisioning:1:cat:B13B3B7B08 6458CFE040E80A19AA560C" -show_folder_id
list_swlib_storage_ locations (Listing Software Library storage locations)	emcli list_swlib_storage_ locations [-type="OmsShared OmsAgent Ht tp Nfs ExtAgent"]	emcli list_swlib_storage_ locations -type="OmsAgent"

Table A-3 (Cont.) Software Library EM CLI Verbs and Their Usage

Verb	Usage	Example
refer_swlib_entity_files (Referring files from a Software Library entity)	emcli refer_swlib_entity_files -entity_rev_id="entity_rev_id" -file="<relative file path>[;<new file name>]"-refer_storage="<storage location name>;<storage type>" [-use_latest_revision]	emcli refer_swlib_entity_files -entity_rev_id="oracle:defaultService:em:provisioning:1:cmp:COMP_Component:SUB_Generic:B1B1880C6A8C62AAE040548C42832D14:0.1" -file="scripts/perl/script1.pl;new_script.pl" -refer_storage="myScripts;Http" -use_latest_revision
reimport_swlib_metadata (Re-Importing Software Library metadata)	emcli reimport_swlib_metadata	emcli reimport_swlib_metadata
remove_swlib_storage_location (Removing a Software Library storage location)	emcli remove_swlib_storage_location -name="src location name" -type="OmsShared OmsAgent Http Nfs ExtAgent" -migrate_to_loc="dest location name" [-migrate_to_type="OmsShared OmsAgent Http Nfs ExtAgent"]	emcli remove_swlib_storage_location -name="myOMSSharedLocation" -type="OmsShared" -migrate_to_loc="myNewAGTLocation" -migrate_to_type="OmsAgent"
update_swlib_entity (Modifying a Software Library entity)	emcli update_swlib_entity -entity_rev_id="entity_rev_id" [-desc="entity_desc"] [-attr="<attr name>:<attr value>"] [-prop="<prop name>:<prop value>"] [-secret_prop="<secret prop name>:<secret prop value>"] [-note="note text"] [-use_latest_revision]	emcli update_swlib_entity -entity_rev_id="oracle:defaultService:em:provisioning:1:cmp:COMP_Component:SUB_Generic:B1B1880C6A8C62AAE040548C4D14:0.1" -entity_desc="myexampleInstall description" -attr="PRODUCT:example" -attr="PRODUCT_VERSION:3.0" -attr="VENDOR:example Corp" -prop="DEFAULT_HOME:/u01/example3/" -note="myexampleInstall for test servers"
upload_swlib_entity_files (Uploading files to a Software Library entity)	emcli upload_swlib_entity_files -entity_rev_id="entity_rev_id" -file="<abs file path>[;<new file name>]"-host="hostname" [-credential_set_name="setname"] [-credential_name="name" -credential_owner="owner"] [-upload_storage="<storage location name>;<storage type>"] [-use_latest_revision]	emcli upload_swlib_entity_files -entity_rev_id="oracle:defaultService:em:provisioning:1:cmp:COMP_Component:SUB_Generic:B1B1880C6A8C62AAE040548C42832D14:0.1" -file="/u01/example_downloads/file1.zip;newfile1.zip" -file="/u01/example_downloads/file2.zip" -host="fs1.us.example.com" -credential_name="MyexampleCreds" -credential_owner="example_USER" -use_latest_revision

A.4 Provisioning Using EM CLI

Deployment Procedures can be run from the command line using EM CLI or from Cloud Control UI. Launching a procedure either from command line or from GUI requires a set of inputs to be provided. However, the mode of entering these inputs differ in both the cases. While running a Deployment Procedure from the UI, you can use a wizard to enter all the inputs required to run the procedure. However, in EM CLI, you use Properties File for entering the inputs. Properties File is a file which contains all the inputs required to run a Deployment Procedure. The following sections describe how to create properties file from scratch and use it in procedures, how to use properties file of a procedure that has already been executed, and how to create a template using a properties file and a few other attributes to run the deployment procedures.

Note: The `-swlib` argument works for cloning only Oracle Database 9i Release 2. Do NOT use this argument for later releases.

This section covers the following scenarios:

- [Creating the Properties File to Submit a Deployment Procedure](#)
- [Using Properties File from an Existing Execution of a Deployment Procedure](#)
- [Launching a Procedure using an Existing Saved Procedure](#)

A.4.1 Creating the Properties File to Submit a Deployment Procedure

This graphic illustrates how to create a template properties file, update values into the file, and then submit the procedure with the updated properties file as the input.



Step1: Create Template Properties File From a Procedure Definition

All the details required for the selected Deployment Procedure like variable names, targets, credentials, and so on are provided in this step to successfully submit the procedure from the command line. Generating the Properties file is a two-step process as follows:

1. To retrieve the **GUID** or the **Name** of the procedure, run the following command:

```
emcli get_procedures
[-type={procedure type}]
```

Example:

```
./emcli get_procedures -type=DBPROV
```

Output:

```
B3FCE84B1ED96791E040578CD7810EC5, DBPROV, Prov_112_db_using_SH_locked_acc_
without_env_shift_ssubbura11, Prov_112_db_using_SH_locked_acc_without_env_
shift_ssubbura11, 1.0, SSUBBURA1, SIHA_SIDB_PROC
B35E10B1F430B4EEE040578CD78179DC, DBPROV, DBREPLAYCLIENTDP_NG, Provision Oracle
Database Client, 6.1, ORACLE
B35E10B1F427B4EEE040578CD78179DC, DBPROV, SIHA_SIDB_PROC, Provision Oracle
Database, 1.0, ORACLE
```

2. Use the GUID or the name in the following command to generate a template properties file. Use the following command when you are running the Deployment Procedure for the first time, or when you do not have too many variables in your procedure to update:

```
emcli describe_procedure_input
[-procedure={procedure GUID}]
[-name={procedure name or procedure configuration}]
[-owner={owner of the procedure or procedure configuration}][-parent_
proc={procedure of the procedure configuration. this only applies to describe a
procedure configuration with the same name}]
```

The following examples describe how to use the procedure GUID to generate the properties file template:

```
./emcli describe_procedure_input -procedure=B35E10B1F427B4EEE040578CD78179DC >
procConfiguration.properties
```

This EM CLI verb describes the input data of a deployment procedure or a procedure configuration in a name-value pair format, which is also called as the *properties file format*. The advantage of this name-value file format for a procedure is that it is flexible enough to accept multiple destination targets.

Step 2: Entering New Values in The Properties File

Use any editor to open the properties file and enter values against the names. After updating all the fields, save and close the properties file.

The main goal of this step is to create a library of property files where the most common input values have been set as defaults, this in turn reduces the chances of operator errors, and also reduces the number of inputs expected from the operators.

For example, vi procConfiguration.properties

Note: For example properties file, see sections [Section A.6.1](#) or [Section A.6.2](#).

Step 3: Submitting the Procedure With The Updated Properties File as Input

Once the properties file is ready with the correct name-value pair required to run the Deployment procedure, you must use the EM CLI verb *submit_procedure*, which accepts the edited properties file as the input.

```
emcli submit_procedure
[-name={name of the procedure}]
[-owner={owner of the procedure}]
[-procedure={guid of the procedure}]
-input_file={data:{file_path}/file name" [-instance_name={name for the procedure
instance}] [-notification={procedure status}]
[-grants={users and their corresponding accessing levels}] [-schedule=start_
time:yyyy/MM/dd HH:mm; tz:{java timezone ID}]
```

Starting with Cloud Control 12c, you can submit the procedure either using the procedure GUID or using the procedure name/owner pair, as described in the following example:

- Submitting the properties file using the GUID of the procedure:

```
emcli submit_procedure -input_file=data:procConfiguration.properties
-procedure=B35E10B1F427B4EEE040578CD78179DC -schedule="start_time:2006/6/21
21:23; tz:America/New_York" -grants="user1:VIEW_JOB; user2:FULL_JOB"
-notification="scheduled, action required, running"
```

- Submitting the properties file using the procedure name/owner pair:

```
emcli submit_procedure -input_file=data:procConfiguration.properties
-name=SIHA_SIDB_PROC -owner=sysman -schedule="start_time:2006/6/21 21:23;
tz:America/New_York" -grants="user1:VIEW_JOB; user2:FULL_JOB"
-notification="scheduled, action required, running"
```

Output:

```
Verifying parameters ...
B35E10B1F427B4EEE040578CD78179DC
Deployment procedure submitted successfully
Note: The instanceId is B35E10B1F427B4EEE040578CD78179F1
```

This verb functions in a non-waiting mode, which means it submits the procedure for execution and returns without waiting for it to complete. The output of this verb indicates if the submission of the procedure was successful or if any errors were encountered. A successful submission displays the Instance GUID as the output.

Step 4: Verifying The Status Of the Procedure

The final step lets you to track the progress and status of the procedure. This is especially important since the submit procedure verb does not wait for the completion of the Deployment Procedure:

```
emcli get_instance_status
[-instance={instance guid}]
[-exec=execution guid]
[-xml]
[-details]
[-showJobOutput]
[-tailLength={last N characters}]
```

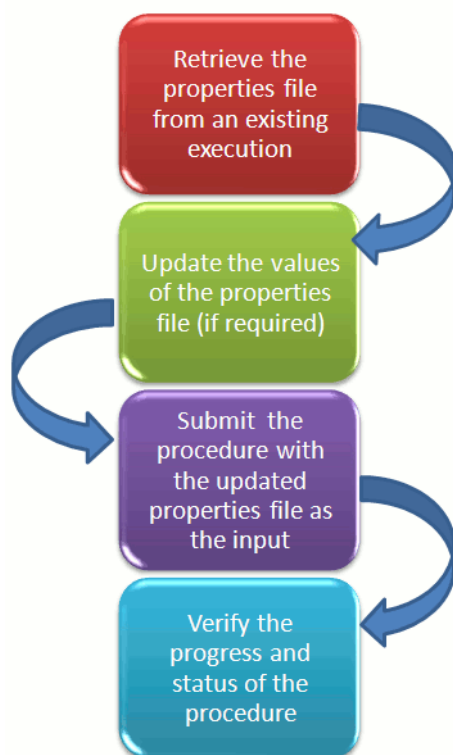
Example:

```
emcli get_instance_status -instance=B35E10B1F427B4EEE040578CD78179F1 -details
-showJobOutput
```

Output:
B35E10B1F427B4EEE040578CD78179F1, WEBLOGIC_WSM, DANS_SCALEUP_WSM12, FAILED

A.4.2 Using Properties File from an Existing Execution of a Deployment Procedure

This graphic illustrates how to retrieve the properties file of a deployment procedure that has already been executed, update values into the file, and then submit the procedure with the updated properties file as the input.



Retrieving Properties File From an Existing Execution

All the inputs required for the selected Deployment Procedure like variable names, targets, credentials, and so on are provided in this step to successfully submit the procedure from the command line. Generating the Properties file is a two-step process as follows:

1. To retrieve the **GUID** or the **Name** of the procedure, run the following command:

```
emcli get_procedures
[-type={procedure type}]
[-parent_proc={procedure associate with procedure configuration}]
```

Example:

```
./emcli get_procedures -parent_proc=SIHA_SIDB_PROC
```

Output:

```
B3FCE84B1ED96791E040578CD7810EC5, DBPROV, Prov_112_db_using_SH_locked_acc_
without_env_shift_ssubbura11, Prov_112_db_using_SH_locked_acc_without_env_
shift_ssubbura11, 1.0, SSUBBURA1, SIHA_SIDB_PROC
```

2. Use the GUID to retrieve the Instance ID of the procedure:

```
emcli get_instances
[-type={procedure type}]
```

Example:

```
./emcli get_instances -type=DBPROV
```

Output:

```
B3FE0C8302EA4A4CE040578CD781133C, B3FE0C8302F64A4CE040578CD781133C, DBPROV,
Prov_112_db_using_SH_locked_acc_without_env_shift_ssubbur, Failed
B3FE34D472C00AD9E040578CD781107B, B3FE34D472CC0AD9E040578CD781107B, DBPROV,
Prov_112_db_using_SH_locked_acc_without_env_shift_ssubbural, Failed
```

3. Use the Instance ID in the following command to retrieve the input properties file of the instance:

```
emcli get_instance_data
[-instance={instance guid}]
[-exec=execution guid]
```

The following examples describe how to use the procedure GUID to generate the properties file template:

```
emcli get_instance_data -instance=B3FE0C8302EA4A4CE040578CD781133C >
instanceData.properties
```

Step 2: Updating the Existing Values in the Properties File

The main goal of this step is to update the values in the properties file (if required). To do so, use any editor to open the properties file and enter the updated values against the names. After updating the required fields, save and close the properties file.

Example:

```
vi instanceData.properties
```

Step 3: Submitting the Procedure with the Updated Properties File as Input

To run the procedures from the command line you must use the EM CLI verb *submit_procedure* as described in [Step 3: Submitting the Procedure With The Updated Properties File as Input](#)

Step 4: Verifying the Status of the Procedure

To verify the status of the procedure, see [Step 4: Verifying The Status Of the Procedure](#).

A.4.3 Launching a Procedure using an Existing Saved Procedure

Procedures that are used repeatedly can be saved along with the properties file, job grants, schedules, and notifications, and so on with a unique name. This specially packaged procedure can be run using the unique name whenever required. This is especially useful when the procedure must be executed multiple number of times, and helps in saving a lot of time and effort. Running the verb `emcli get_procedures` fetches all the procedures which also include the Procedure Configurations.

To launch a procedure using an Existing Procedure Configuration File, do the following:

1. Run the verb `emcli get_procedures` to fetch an existing Procedure Configuration file.

2. Update the properties file if required.
3. Save the Procedure Configuration with the updated Properties file, and the other attributes like job grants, schedules, and notifications. To do so, see [Section A.4.3.1](#).
4. Submitting the Procedure Configuration file as described in [Step 3: Submitting the Procedure With The Updated Properties File as Input](#)

Note: You can update the Procedure Configuration using the `update_procedure_input` verb as described in [Section A.4.3.2](#). After Updating the Procedure Configuration, follow step 4 to resubmit the procedure.

5. To verify the status of the procedure, see [Step 4: Verifying The Status Of the Procedure](#).

A.4.3.1 Saving a Procedure Configuration of a Procedure

If you have to use a properties file repeatedly to run a procedure, then Oracle recommends that you save this Procedure with the properties file and give the saved procedure a name. Every time you want to run the procedure with the same properties file, you can run the saved Procedure by giving its name. To save the procedure, run the following command:

```
emcli save_procedure_input -name={name of procedure configuration}
-procedure={Procedure name}
[-owner={owner of procedure}]
-input_file=data:/file path/file name
[-grants={users and their corresponding accessing levels}]
[-notification={procedure status}]
[-schedule=start_time:yyyy/MM/dd HH:mm;tz:{java timezone id};grace_period:xxx]
```

Example:

```
emcli save_procedure_input -name=procConfiguration -procedure=ComputeStepTest
-input_file=data:/tmp/instanceData.properties -grants="user1:VIEW_JOB;
user2:FULL_JOB" -notification="scheduled, action required, running"
-schedule="start_time:2012/12/25 00:00;tz:American/New York;grace_period:60"
```

A.4.3.2 Updating the Procedure Configuration of a Procedure

To update the existing values in a saved procedure, run the following command:

```
emcli update_procedure_input -name={name of procedure configuration} -input_
file="data:/file path/file name"
[-notification={procedure status}]
[-grants={users and their corresponding accessing levels}]
[-schedule=start_time:yyyy/MM/dd HH:mm;tz:{java timezone id};grace_period:xxx]
```

Example:

```
emcli update_procedure_input -name=procConfiguration -input_
file=data:/tmp/instanceData.properties -grants="user1:VIEW_JOB;user2:FULL_JOB"
-notification="scheduled, action required, running" -schedule="start_
time:2012/12/25 00:00;tz:American/New York;grace_period:60"
```

A.5 Patching Using EM CLI

This section contains the following:

- [Before You Begin](#)

- [Patching Using EM CLI](#)

A.5.1 Before You Begin

Keep the following points in mind before patching the targets using EM CLI:

1. Target information like : target name, target type, target version, release number, platform, product and so on ready.
2. Patch information like: Patch Name (Patch Number), Release ID, Platform ID, and Language ID ready.
3. Set at least one of the following credentials on the Oracle home of the target host machines before beginning the patching process:
 - Oracle Home Named Credentials
 - Privileged Oracle Home Named Credentials
4. Setup Privilege Delegation through Sudo or PowerBroker, and apply the templates to the host target when you do not have the access (Username/Password) for the `Oracle` account or `root` account.
5. Set one of the following modes before patching:
 - **Online Mode:** This mode is helpful when you have internet connectivity. However, to search and download the patches from *My Oracle Support*, you need to set the preferred credentials for *My Oracle Support*.
 - **Offline Mode:** This mode can be used for patching provided you have already downloaded the patches to the Software Library. You can then search for them on Software Library.

A.5.2 Patching Using EM CLI

Starting with Enterprise Manager 12c, targets can be patched using Enterprise Manager Command Line Interface. You do not necessarily need Cloud Control to download and apply patches.

The following table describes EM CLI patching scenarios:

Table A-4 EM CLI Patching Scenarios

Case No	Scenario	High Level Steps
Case 1	Creating a new properties file for patching targets.	<p>To patch targets using a fresh properties file, follow these steps:</p> <ol style="list-style-type: none"> 1. Select the targets, and search for the patches that you want to add to the plan. 2. Create a properties file, and save it in a temporary location. 3. Create the plan using the properties file as the input. 4. View the patch plan before submitting to know if the given patch plan can be submitted. If the action is : <ul style="list-style-type: none"> - Analyze, then you can submit your patch plan for analysis. - Deploy, then you can submit your patch plan for deployment. 5. Verify the status of the submitted plan. <p>For details about how to use the EM CLI commands to perform each of the steps see Section A.5.2.1.</p>
Case 2	Updating the properties file of an existing patch plan to patch the targets.	<p>To update a properties file retrieved from an existing patch plan, follow these steps:</p> <ol style="list-style-type: none"> 1. Get the user-editable data for a given patch plan, and save the output as a properties file. 2. Edit the properties file using an editor. For example, vi editor. 3. Save the edited user-data. 4. View the patch plan before submitting to know if the given patch plan can be submitted. If the action is : <ul style="list-style-type: none"> - Analyze, then you can submit your patch plan for analysis. - Deploy, then you can submit your patch plan for deployment. 5. Verify the status of the submitted plan. <p>For details about how to use the EMCLI commands to perform each of the steps see Section A.5.2.2.</p>

A.5.2.1 Creating a New Properties File for Patching Targets

If you are creating the patch plan from scratch, then you need to create the properties file afresh, and submit this properties file as input for creating the plan. To do so, follow these steps:

1. Select the targets that need to be patched. To do so, run the following EM CLI command:

```
emcli get_targets
      [-targets=" [name1:]type1; [name2:]type2; ... "]
```

For example:

```
emcli get_targets -targets=oracle_emd
```

Output:

Displays all the Management Agent targets.

Status ID	Status	Target Type	Target Name
2	Metric collection on Error	oracle_emd	h1.us.example.com:5125
2	Metric collection on Error	oracle_emd	h2.us.example.com:5125
1	Up	oracle_emd	slc01nha.us.example.com:11852
1	Up	oracle_emd	slc00bng.us.example.com:1833
1	Up	oracle_emd	adc2101349.us.example.com:1832

2. Search for the patches that you want to apply. To find the relevant patches for your plan, you either need to use the Patch ID (Basic Search), or use a combination of Release ID, Platform ID, and Product ID (Advanced Search) and drill down to the patches required. To do so, run the following EM CLI command:

```
emcli search_patches
  [-swlib]
  [-patch_name="patch_name"]
  [-product="product id" [-include_all_products_in_family]]
  [-release="release id"]
  [-platform="platform id" | -language="language id"]
  [-type="patch | patchset"]
  [-noheader]
  [-script | -xml | -format=
                                [name:<pretty|script|csv>;
                                [column_separator:"column_sep_string"];
                                [row_separator:"row_sep_string"];
  ]
```

Note: You can search for patches in one of the following locations:

- ARU Site
- Software Library

If you have internet connectivity, then you are in online mode, and by default can look for patches on the ARU site. However, if you are in offline mode, then you must ensure that the patches are already uploaded to Software Library so you can use them.

You can perform searches in one of the following modes using EM CLI:

- Simple Search: This mode allows you to search the ARU site or Software Library using the patch ID information.
- Advanced Search: This mode allows you to provide a combination of key values like platform ID, Language ID, Release ID, and/or product ID to drill down to the patch that you are looking for.

You can use the following syntax, and the corresponding examples to perform simple and advanced search using EM CLI commands:

- a. (*Basic Search*) To search for the patches using the **Patch ID**, do the following:


```

emcli search_patches
    [-swlib]
    [-patch_name="patch_name"]
    [-product="product id" [-include_all_products_in_family]]
    [-release="release id"]
    [-platform="platform id" | -language="language id"]
    [-type="patch | patchset"]
    [-noheader]
    [-script | -xml | -format=
                                     [name:<pretty|script|csv>];
                                     [column_separator:"column_sep_string"];
                                     [row_separator:"row_sep_string"];
    ]

```

Example 1: Basic Search (Online Mode)

To search for patches on My Oracle Support using the Patch ID:

```
emcli search_patches -patch_name=11993573
```

Output:

```

11993573      Agent Plugin PATCH      Cloud Control (Agent) 12.1.0.1.0
Linux x86-64  American English      General Enterprise Manager Base
Platform - Plugin

```

Example 2: Basic Search (Offline Mode)

To search for patches on Software Library using the patch ID:

```
emcli search_patches -patch_name=11993573 -swlib -script
```

Output:

```

11993573      Agent Plugin PATCH      Cloud Control (Agent) 12.1.0.1.0
Linux x86-64  American English      General Enterprise Manager Base
Platform - Plugin

```

- b. (Advanced Search) Use the Product ID, Release ID, and Platform ID (or Language ID) to get the patch details that you want to add to the patch plan.**

Example:

To search for patches using a combination of Product ID, Release ID, and Platform ID (obtained from the earlier steps):

```
emcli search_patches -product=12383 -release=9800371121010 -platform=226
```

Output:

```

13491785      ENTERPRISE MANAGER BASE PLATFORM - AGENT 12.1.0.1.0 BP1
(PORT) Cloud Control (Agent) 12.1.0.1.0      Linux x86-64  American
English      Recommended      Enterprise Manager Base Platform13481721
WRONG ERROR MESSAGE RETURNED FROM NMO      Cloud Control (Agent) 12.1.0.1.0
Linux x86-64  American English      General Enterprise Manager Base
Platform

```

- 3. Create a patch-target map (stored in the properties file) using any editor, and supply information like Patch ID, Release ID, Platform ID, and Language ID. Here is a sample properties file:**

```
vi demo.props
```

```

patch.0.patch_id=13426630
patch.0.release_id=9800371121010
patch.0.platform_id=2000
patch.0.language_id=0
patch.0.target_name=slc00bng.us.example.com:1836
patch.0.target_type=oracle_emd
patch.1.patch_id=13426630
patch.1.release_id=9800371121010

```

```
patch.1.platform_id=2000
patch.1.language_id=0
patch.1.target_name=slc01nha.us.example.com:1839
patch.1.target_type=oracle_emd
```

4. Run the `create_patch_plan` command to create the plan, and supply the newly created properties file (`demo.props`) as input:

```
emcli create_patch_plan
  -name="name"
  -input_file=data:"file_path"
  [-impact_other_targets="add_all | add_original_only | cancel"]
```

Example:

```
emcli create_patch_plan -name=demo_agent -input_file=data:demo.props -impact_
other_targets=add_all
```

Note: If the selected target impacts other targets, then you need to add `impact_other_targets` with the value "add_all". For example, if one of the agents running on the NFS home is selected for patching, other agent based on the same NFS home will also be impacted while patching, so they are all required to present in the patch plan.

5. After you have created the patch plan with all the relevant data, you can submit your patch plan in the Analyze mode to verify if the plan is deployable or not. To do so, run the following command:

```
emcli submit_patch_plan -name=demo_agent -action=analyze
```

Output:

```
The action "analyze" is successfully submitted on the Patch Plan "demo_agent",
now "analyze" is in progress.
```

The **Analyze** mode facilitates the plan to perform all the validations to ensure that the plan is deployable. Only once the analysis is successful you should deploy the plan.

6. To verify the status of the patch plan, run the following EM CLI command:

```
emcli show_patch_plan -name=demo_agent -info | grep plan_status
```

Output:

```
<plan_status>CONFLICTS</plan_status>
```

If you see any conflicts, then you must resolve them before deploying the plan. You can use the User Interface to resolve the issues, and then rerun the plan until the status is **CLEAN**.

7. After a successful analysis, you can deploy the patch plan. To do so, run the following command with action **deploy**:

```
emcli submit_patch_plan -name=agent_demo -action=deploy
```

Output:

```
The action "deploy" is successfully submitted on the Patch Plan "demo_agent",
now "deploy" is in progress
```

- To verify the status of the plan, run the EM CLI command `show_patch_plan` as mentioned in step 6. Only when the output of the command is `DEPLOY_SUCCESS`, it means that the plan has been successfully deployed, and the targets mentioned in the patch plan have been patched.

```
emcli show_patch_plan -name=demo_agent -info
```

Output:

```
<plan>
  <planDetails>
    <plan_id>79CAF6A6DAFCFEE6654C425632F19411</plan_id>
    <name>demo</name>
    <type>PATCH</type>
    <description/>
    <conflict_check_date>Tue Feb 21 18:04:04 PST 2012</conflict_check_date>
    <conflict_check_date_ms>1329876244000</conflict_check_date_ms>
    <is_deployable>1</is_deployable>
    <plan_status>CONFLICTS</plan_status>
    <review_status>CONFLICT_FREE</review_status>
    <created_date>Tue Feb 21 17:40:47 PST 2012</created_date>
    <created_date_ms>1329874847000</created_date_ms>
    <created_by>SYSMAN</created_by>
    <last_updated_date>Tue Feb 21 17:58:29 PST 2012</last_updated_date>
    <last_updated_date_ms>1329875909000</last_updated_date_ms>
    <last_updated_by>SYSMAN</last_updated_by>
    <grant_priv>yes</grant_priv>
    <user_plan_privilege>FULL</user_plan_privilege>
    <see_all_targets>N</see_all_targets>
    <homogeneousGroupLabel>Database Instance 10.2.0.1.0 (Linux
x86-64)</homogeneousGroupLabel>
    <executeGuid/>
    <executeUrl/>
  </planDetails/>
```

- To get the details of the patching procedure/job that you submitted, use the GUID of the execution in the command `get_job_execution_details` as follows:

```
emcli get_job_execution_detail
  -execution={execution_id}
  [-xml [-showOutput [-tailLength={length}]]]
```

For Example:

```
emcli get_job_execution_detail -execution=79CAF6A6DAFCFEE6654C425632F19411 -xml
```

A.5.2.2 Using the Properties File of an Existing Patch Plan to Patch the targets

To edit an existing patch plan after it has been created for updating the patch-target pairs or generic information or deployment options, you can follow the steps listed here:

- To view the user-editable fields of an existing plan, run the `get_patch_plan_data` command, and save the output to a properties file as follows:

```
$ emcli get_patch_plan_data -name=demo_agent >demo_agent.props
```

Output:

```
name=demo_agent
description=
deployment_date=
planPrivilegeList=VIEWER:ADMIN:VIEW;OPER:ADMIN:VIEW;DESIGNER:ADMIN:VIEW
```

```

patch.0.patch_id=13426630
patch.0.release_id=9800371121010
patch.0.platform_id=2000
patch.0.language_id=0
patch.0.target_name=slc00bng.us.example.com:1836
patch.0.target_type=oracle_emd
patch.1.patch_id=13426630
patch.1.release_id=9800371121010
patch.1.platform_id=2000
patch.1.language_id=0
patch.1.target_name=slc00aoe.us.example.com:4473
patch.1.target_type=oracle_emd
deploymentOptions.StageLocation=%emd_emstagedir%
deploymentOptions.AdvancedOPatchOptions=null
deploymentOptions.StagePatches=true

```

2. Edit the properties file (`demo_agent.props`) using any editor. You can change the storage location as follows:

```

name=demo_agent
description=
deployment_date=
planPrivilegeList=VIEWER:ADMIN:VIEW;OPER:ADMIN:VIEW;DESIGNER:ADMIN:VIEW
patch.0.patch_id=13426630
patch.0.release_id=9800371121010
patch.0.platform_id=2000
patch.0.language_id=0
patch.0.target_name=slc00bng.us.example.com:1836
patch.0.target_type=oracle_emd
patch.1.patch_id=13426630
patch.1.release_id=9800371121010
patch.1.platform_id=2000
patch.1.language_id=0
patch.1.target_name=slc00aoe.us.example.com:4473
patch.1.target_type=oracle_emd
deploymentOptions.StageLocation=%emd_emstagedir%/demo
deploymentOptions.AdvancedOPatchOptions=null
deploymentOptions.StagePatches=true

```

3. To save the patch plan with the new edited data, run `set_patch_plan_data` command as follows:

```
emcli set_patch_plan_data -name=demo_agent -input_file=data:demo_agent.props
```

Output:

It is successfully on updating deployment options from the patch plan.

Note: If the selected target impacts other targets, then you need to add `impact_other_targets` with the value "add_all". For example, if one of the agents running on the NFS home is selected for patching, other agent based on the same NFS home will also be impacted while patching, so they are all required to present in the patch plan.

4. Follow steps 5, 6, 7, 8, and 9 mentioned in the [Section A.5.2.1](#) to complete the patching process.

A.6 WorkFlow Examples Using EM CLI Commands

The following sections describe some of the provisioning, patching, and Software Library tasks that can be performed using EM CLI commands:

- [Provisioning Oracle Database Software](#)
- [Provisioning Oracle WebLogic Server](#)
- [Provisioning User Defined Deployment Procedure](#)
- [Patching WebLogic Server Target](#)
- [Creating a New Generic Component by Associating a Zip File](#)

A.6.1 Provisioning Oracle Database Software

This use case describes how to provision an Oracle Database Software using the EM CLI commands available in Cloud Control. The first step is to filter out the database procedures running in your enterprise, from the list, select the Single Instance Database procedure and its corresponding GUID. For the SI DB procedure, a new properties file is created from scratch. Initially, the name-value pair in the template will be empty, you must edit the attributes in the properties file to update the values. Following which the procedure is submitted with the updated properties file as the input, and tracked to completion.

Note: The following verb clones only Oracle Database 9i Release 2:
emcli clone_database_home -swlib true.

Here is the step-by-step procedure with the outputs:

1. To retrieve the GUID of the Deployment Procedure, run the following command:

```
./emcli get_procedures | grep DB_
```

For Example:

```
./emcli get_procedures | grep DB
B3F.CE84B1ED96791E040578CD7810EC5, DBPROV, Prov_112_db_using_SH_locked_acc_
without_env_shift_ssubbura11, Prov_112_db_using_SH_locked_acc_without_env_
shift_ssubbura11, 1.0, SSUBBURA1, SIHA_SIDB_PROC
B35E10B1F42AB4EEE040578CD78179DC, DB_PROV_UPGRADE, DbProvUpgradeDP, Upgrade
Oracle Database, 1.0, ORACLE
B35E10B1F427B4EEE040578CD78179DC, DBPROV, SIHA_SIDB_PROC, Provision Oracle
Database, 1.0, ORACLE
```

Select the GUID corresponding to the SIHA_SIDB_PROC , which is
B35E10B1F427B4EEE040578CD78179DC

2. Create the Properties File template using the following command:

```
./emcli describe_procedure_input -procedure=B35E10B1F427B4EEE040578CD78179DC >
sihasidb.properties
```

3. Use an editor to open the generated properties file sihasidb.properties file, and enter the required values.

For example, here is a sample properties file used with the values updated in them:

```
# The Procedure Configuration with name emcli_11202 has input and arguments as
follows:
```

```
# Input properties are:
DB_COMPONENT=11SSUBBURA/Oracle Database Installation Media
DB_HOST_NORMAL_CREDNAMES=AIME_USER1:PGURUSWA1
DB_HOST_ROOT_CREDNAMES=AIME_ROOT:PGURUSWA1
DB_ORACLE_BASE_LOC=/scratch/db11202
DB_ORACLE_HOME_LOC=/scratch/db11202/app/product/11.2.0/db
DB_PRODUCT_VERSION=11.2.0.2.0
DEPLOY_MODE=DEPLOY_DB
OINSTALL_GROUP=svrtech
OSDBA_GROUP=dba
OSOPER_GROUP=oper
PAUSE_AFTER_PREREQ=false
RAC_HOME_SHARED=false
SOURCE_TYPE=SOFTWARE_LIBRARY
TARGET_HOST_LIST=sta123.us.example.com
WORK_DIR_LOC=/tmp
```

4. Submit the procedure using the following command:

```
./emcli submit_procedure -input_file=data:sihasidb.properties
-instance="emcli_db1" -procedure=B35E10B1F427B4EEE040578CD78179DC
Verifying parameters ...
Schedule not specified, defaults to immediate
A8F7700333BAE9FAE040E40A45D866F1
Deployment procedure submitted successfully
```

A.6.2 Provisioning Oracle WebLogic Server

This use case describes how to provision an Oracle WebLogic Server, and how to Scale up and Scale out Middleware procedures using the EM CLI commands available in Cloud Control.

Cloud Control supports the following usecases for provisioning Oracle WebLogic Server using EM CLI commands:

- [Provisioning Oracle WebLogic Server Using the Provisioning Profile](#)
- [Scaling Up or Scaling Out Middleware Deployment Procedure](#)

Prerequisites

- Ensure that you have setup a WebLogic Domain with Administrator Server and Managed Server, and registered your targets with the OMS so that your host target is discovered on the Middleware Provisioning Page.
- Create the WebLogic Domain Provisioning Profile, this ensures that the domain selected and its Middleware Home are archived and stored in the software library for future cloning operations. You can use this profile while cloning a WebLogic domain.

Provisioning Oracle WebLogic Server Using the Provisioning Profile

The first step is to filter out the FMW procedures running in your enterprise, from the list, select the `FMWPROV` procedure and its corresponding GUID. For the `FMWPROV` procedure, a new properties file template is created from scratch. Initially, the name-value pair in the template will be empty, you must edit the attributes in the properties file to update the values. Following which the procedure is submitted with the updated properties file as the input, and tracked to completion.

Follow these steps:

1. To retrieve the GUID of the Deployment Procedure, run the following command:

```
./emcli get_procedures | grep FMWPROV_
```

The output appears in the following format:

```
<proc_guid>, <procedure_type>, <Procedure_name>, <Display name>, <version>,
<Parent procedure name>
```

For example:

```
./emcli get_procedures | grep FMWPROV_
B35E10B1F154B4EEE040578CD78179DC, FMW Provisioning, FMWPROV_DP, Provision
Middleware, 2.0, ORACLE
```

2. Use the GUID retrieved in the previous step to prepare the Properties File template using the following command:

```
./emcli describe_procedure_input - procedure=<proc_guid> -name = <proc_name>
```

For example:

```
./emcli describe_procedure_input -procedure=B35E10B1F154B4EEE040578CD78179DC >
instanceFMWData.properties
A properties file with the name instanceFMWData.properties is created
```

3. Use an editor to open the generated properties file *instanceFMWData.properties*, and enter the required values.

For example, here is a sample properties file used with the values updated in them:

```
# Input properties are:
```

```
APPS_GOLD_IMAGE_FILENAME=apps.zip
ARCHIVE_FILE_NAME=archive.jar
CLONING_JAR_NAME=cloningclient.jar
CONFIG_PLAN_OBJECT_DP_VARIABLE=Type:JDBCSystemResource;Action:Set;
Attributes[Name:mds-owsm~Target:Cluster_1,Cluster_2]<BR>
CREATE_DOMAIN=true
DEST_ADMIN_HOST.0.ADMIN_SQL_HOME=
DEST_ADMIN_HOST.0.DATASOURCE_PROPERTY_FILE_DIR=
DEST_ADMIN_HOST.0.DATASOURCE_PROPERTY_FILE_NAME=
DEST_ADMIN_HOST.0.DOMAIN_HOME_DEST_ADMIN_HOST=/scratch/FFT4_EMCLI
DEST_ADMIN_HOST.0.DOMAIN_NAME_DEST_ADMIN_HOST=FFT4_EMCLI
DEST_ADMIN_HOST.0.FMW_HOME_DEST_ADMIN_HOST=/scratch/fmwprov
DEST_ADMIN_HOST.0.HAS_MANAGED_SERVER_REMOTE=false
DEST_ADMIN_HOST.0.MS_TEMPLATE_DEST_ADMIN_HOST=testMA.jar
DEST_ADMIN_HOST.0.MS_TEMPLATE_NAME=mytemplate
DEST_ADMIN_HOST.0.ORACLE_HOME_DEST_ADMIN_HOST=
DEST_ADMIN_HOST.0.PORT_DETAILS_DEST_ADMIN_HOST=7001:Listen Port,7002:SSL Listen
Port
DEST_ADMIN_HOST.0.PRODUCT_TYPE_DEST_ADMIN_HOST=SOA
DEST_ADMIN_HOST.0.SERVER_NAME_DEST_ADMIN_HOST=AdminServer
DEST_ADMIN_HOST.0.START_SERVER_REQUIRED_DEST_ADMIN_HOST=true
DEST_ADMIN_HOST.0.WLS_HOME_DEST_ADMIN_HOST=/scratch/fmwprov/wlserver_10.3
DEST_ADMIN_HOST.0.WLS_PASSWORD_DEST_ADMIN_HOST=welcome1
DEST_ADMIN_HOST.0.WLS_USERNAME_DEST_ADMIN_HOST=weblogic
DEST_ADMIN_HOST.0.WORK_DIR_LOC_DEST_ADMIN_HOST=/tmp/fmwProvDest
DEST_ADMIN_HOST.0.defaultHostCred=PREF:HostCredsNormal
DEST_ADMIN_HOST.0.name=slc00ave.us.example.com
DEST_ADMIN_HOST.0.type=host
DEST_ADMIN_HOST_NAME=slc00ave.us.example.com
DEST_ADMIN_PORT=7001
DEST_ADMIN_WORK_DIR_LOC=/tmp/fmwProvDest
```

```

DEST_FMW_HOST.0.FMW_HOME_DEST_FMW_HOST=/scratch/fmwprov
DEST_FMW_HOST.0.JDK_HOME_DEST_FMW_HOST=
DEST_FMW_HOST.0.JRE_LOC=%emd_root%/jdk
DEST_FMW_HOST.0.LOG_DIR=
DEST_FMW_HOST.0.ORACLE_HOME_DEST_FMW_HOST=
DEST_FMW_HOST.0.OUI_HOME=
DEST_FMW_HOST.0.PREREQ_PATH=
DEST_FMW_HOST.0.WLS_HOME_DEST_FMW_HOST=/scratch/fmwprov/wlserver_10.3
DEST_FMW_HOST.0.WORK_DIR_LOC_DEST_FMW_HOST=/tmp/fmwProvDest
DEST_FMW_HOST.0.defaultHostCred=PREF:HostCredsNormal
DEST_FMW_HOST.0.name=slc00ave.us.example.com
DEST_FMW_HOST.0.type=host
DEST_MANAGED_SERVERS.0.ADMIN_HOST_NAME_DEST_MANAGED_
SERVERS=slc00ave.us.example.com
DEST_MANAGED_SERVERS.0.ADMIN_HOST_PASSWORD_DEST_MANAGED_SERVERS=welcome1
DEST_MANAGED_SERVERS.0.ADMIN_HOST_USERNAME_DEST_MANAGED_SERVERS=weblogic
DEST_MANAGED_SERVERS.0.ADMIN_PORT_DEST_MANAGED_SERVERS=7001
DEST_MANAGED_SERVERS.0.DOMAIN_HOME_DEST_MANAGED_SERVERS=/scratch/FFT4_EMCLI
DEST_MANAGED_SERVERS.0.FMW_HOME_DEST_MANAGED_SERVERS=/scratch/fmwprov
DEST_MANAGED_SERVERS.0.MACHINE_NAME_DEST_MANAGED_SERVERS=Machine_1
DEST_MANAGED_SERVERS.0.MANAGED_SERVER_REMOTE_DEST_MANAGED_SERVERS=false
DEST_MANAGED_SERVERS.0.MS_PORT_DETAILS_DEST_MANAGED_SERVERS=9001:Listen
Port,9002:SSL Listen Port
DEST_MANAGED_SERVERS.0.MS_TEMPLATE_DEST_MANAGED_SERVERS=testMA.jar
DEST_MANAGED_SERVERS.0.NM_LISTEN_ADDRESS=localhost
DEST_MANAGED_SERVERS.0.NM_LISTEN_PORT=5556
DEST_MANAGED_SERVERS.0.NM_PORT_DETAILS_DEST_MANAGED_SERVERS=5556:Listen Port
DEST_MANAGED_SERVERS.0.ORACLE_HOME_DEST_MANAGED_SERVERS=
DEST_MANAGED_SERVERS.0.SERVER_NAME_DEST_MANAGED_SERVERS=bam_server1
DEST_MANAGED_SERVERS.0.START_NM=true
DEST_MANAGED_SERVERS.0.START_SERVER_REQUIRED_DEST_MANAGED_SERVERS=true
DEST_MANAGED_SERVERS.0.WLS_HOME_DEST_MANAGED_SERVERS=/scratch/fmwprov/wlserver_
10.3
DEST_MANAGED_SERVERS.0.WORK_DIR_LOC_DEST_MANAGED_SERVERS=/tmp/fmwProvDest
DEST_MANAGED_SERVERS.0.defaultHostCred=PREF:HostCredsNormal
DEST_MANAGED_SERVERS.0.name=slc00ave.us.example.com
DEST_MANAGED_SERVERS.0.type=host
DEST_MANAGED_SERVERS.1.ADMIN_HOST_NAME_DEST_MANAGED_
SERVERS=slc00ave.us.example.com
DEST_MANAGED_SERVERS.1.ADMIN_HOST_PASSWORD_DEST_MANAGED_SERVERS=welcome1
DEST_MANAGED_SERVERS.1.ADMIN_HOST_USERNAME_DEST_MANAGED_SERVERS=weblogic
DEST_MANAGED_SERVERS.1.ADMIN_PORT_DEST_MANAGED_SERVERS=7001
DEST_MANAGED_SERVERS.1.DOMAIN_HOME_DEST_MANAGED_SERVERS=/scratch/FFT4_EMCLI
DEST_MANAGED_SERVERS.1.FMW_HOME_DEST_MANAGED_SERVERS=/scratch/fmwprov
DEST_MANAGED_SERVERS.1.MACHINE_NAME_DEST_MANAGED_SERVERS=
DEST_MANAGED_SERVERS.1.MANAGED_SERVER_REMOTE_DEST_MANAGED_SERVERS=false
DEST_MANAGED_SERVERS.1.MS_PORT_DETAILS_DEST_MANAGED_SERVERS=8001:Listen
Port,8002:SSL Listen Port
DEST_MANAGED_SERVERS.1.MS_TEMPLATE_DEST_MANAGED_SERVERS=testMA.jar
DEST_MANAGED_SERVERS.1.NM_LISTEN_ADDRESS=
DEST_MANAGED_SERVERS.1.NM_LISTEN_PORT=
DEST_MANAGED_SERVERS.1.NM_PORT_DETAILS_DEST_MANAGED_SERVERS=
DEST_MANAGED_SERVERS.1.ORACLE_HOME_DEST_MANAGED_SERVERS=
DEST_MANAGED_SERVERS.1.SERVER_NAME_DEST_MANAGED_SERVERS=soa_server1
DEST_MANAGED_SERVERS.1.START_NM=false
DEST_MANAGED_SERVERS.1.START_SERVER_REQUIRED_DEST_MANAGED_SERVERS=true
DEST_MANAGED_SERVERS.1.WLS_HOME_DEST_MANAGED_SERVERS=/scratch/fmwprov/wlserver_
10.3
DEST_MANAGED_SERVERS.1.WORK_DIR_LOC_DEST_MANAGED_SERVERS=/tmp/fmwProvDest
DEST_MANAGED_SERVERS.1.defaultHostCred=PREF:HostCredsNormal

```



```

DEST_MANAGED_SERVERS.1.name=slc00ave.us.example.com
DEST_MANAGED_SERVERS.1.type=host
DEST_TEMPLATE_FILE_NAME=testMA.jar
DOMAIN_GOLD_IMAGE_FILENAME=DomainTemplate.jar
DO_EXTERNAL_APPS=false
DO_SQL_SCRIPTS=false
EXTRA_FILES_ARCHIVE=extra_files.jar
FARM_PREFIX=Farm01_EMCLI
FMWPROV_ISCLONE=false
FMWPROV_ISDBPROV=false
FMWPROV_ISGOLD=true
FMWPROV_ISINSTALL=false
FMW_COMPONENT=DANS_FFT4/Dans_FFT4_GI_FMWHome
FMW_COMPONENT_FILE=archive.jar
GOLD_IMAGE_FILE_NAME=archive.jar
INSTALL_FMW=true
INSTALL_PRODUCT=false
INSTALL_RCU=false
IS_EXTERNAL_FILE=false
NOT_WINDOWS=true
PREREQ_ONLY_DP=false
PROVISION_MODE=GOLD
RCU_COMPONENT=n/a
REF_SIZE_FILE=sizeprereq
REF_TARGET_ZIP=prereq.zip
REF_TEMPLATE_FILE_NAME=template.jar
REF_TEMPLATE_NAME=mytemplate
RUNNING_WITH_INTERVIEW=true
RUN_RCU=false
SECURE_CONFIG_
PROPERTIES=. PasswordEncrypted:welcome1,welcome1,welcome1,welcome1,welcome1,welc
ome1,welcome1,welcome1
SESSION_TS_LOC=//20110711090737
SIZE_STRING=mw_home_size=1635861705,work_dir_size=3271723410
SQL_ARCHIVE_FILE_NAME=sql-files.zip
START_MODE=ALL
TEMPLATE_COMPONENT=DANS_FFT4/Dans_FFT4_GI_Domain
TEMPLATE_COMPONENT_FILE=DomainTemplate.jar
USE_OWNER_CREDENTIALS=true
USE_SHARED_FMW_HOME=false

```

4. Submit the procedure with the generated instanceFMWData.properties properties file as the input:

```

emcli submit_procedure -input_file=data:<input_properties_file>
-procedure=<proc_guid> -instance_name=<optional_DP_Instance_Name>

./emcli submit_procedure -input_file=data:instanceFMWData.properties
-procedure=B35E10B1F154B4EEE040578CD78179DC

```

Scaling Up or Scaling Out Middleware Deployment Procedure

The process of increasing a cluster's capacity by adding additional server instances to the cluster on an existing machine, or adding machines to the cluster to host the new server instance, is called Scaling up. Scaling Up and Scaling Out Managed Server can be achieved through the command line using EM CLI commands available in Enterprise Manager 12c.

In this use case, the Instance GUID of the SCALEUP procedure is retrieved, which in turn is used to retrieve the input properties file of this instance of the procedure. After

making necessary updates to the properties file, like adding another user-friendly so on, the procedure is submitted with the updated properties file as the input:

Here is the step-by-step process:

1. To retrieve the GUID of the Deployment Procedure, run the following command:

```
./emcli get_procedures | grep SCALEUP_
```

The output appears in the following format:

```
<proc_guid>, <procedure_type>, <Procedure_name>, <Display name>, <version>,
<Parent procedure name>
```

For example:

```
./emcli get_procedure | grep SCALEUP
B35E10B1F154B4EEE040578CD78179DC, FMW Provisioning, SCALEUP DP, Scale up/Scale
out Middleware, 2.0, ORACLE
```

2. Use the Instance GUID retrieved in the previous step to get input properties of an instance of the procedure:

```
./emcli get_instance_data -instance=<instance_guid> -exec=<execution_guid>
```

For example:

```
emcli get_instance_data -instance=B35E10B1F140B4EEE040578CD78179DC >
instanceData.properties
A properties file with the name instanceData.properties is created.
```

Note: This step is valid only if the instances of the procedure is available, which means that the procedure should have been submitted at least once in the past. If you have never submitted the procedure, then you may see an error message as follows:

```
Instance with GUID=<guid> is not found in repository. Please
make sure the value is correct and try again.
```

3. Use an editor to open the generated properties file `instanceData.properties`, and update the existing values in the properties file.
4. Submit the procedure with the generated properties file as the input:

```
./emcli submit_procedure -input_file=data:<input_properties_file>
-procedure=<proc_guid> -instance_name=<optional_DP_Instance_Name>
```

```
./emcli submit_procedure -input_file=data:instanceData.properties
-procedure=B35E10B1F140B4EEE040578CD78179DC
```

A.6.3 Provisioning User Defined Deployment Procedure

This use case describes how to provision a User Defined Deployment Procedure (UDDP) using the EM CLI commands available in Cloud Control. This use case essentially covers, creating the UDDP using the Cloud Control UI, and then submitting the UDDP using the EM CLI commands.

In this use case, a User Defined Deployment Procedure to provision JRE6 on a linux host `abc.example.com` is created using the Cloud Control UI. Steps like **Transfer JRE** and **Check JRE Version** are added to the procedure, and the procedure is submitted with a unique submission name. EM CLI command is then used to retrieve the

instance GUID of the procedure submitted. Minor modifications are made to the properties file, and then submitted through EM CLI.

A.6.3.1 Prerequisites

Ensure that you meet the following prerequisites:

- Log in to Cloud Control as a designer.
- Create Software Library directive to install JRE6 on Linux in the following directory: `/software_library/provisioning/install_jre6_linux32`. Note, you can choose any directory that you want.
- Create Software Library component containing hotspot JRE6 for Linux in the following directory: `/software_library/provisioning/hotspot_jre6_linux32`.

A.6.3.2 Adding Steps and Phases to User Defined Deployment Procedure Using GUI

To add phases and steps to User Defined Deployment Procedure (UDDP), log in to Cloud Control as a Designer, and follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Provisioning and Patching**, then select **Procedure Library**.
2. On the Provisioning page, from the **Actions** menu select **Create New**, and click **Go**.
3. Provide a unique name for your procedure **UDDPTest**, and click **Procedure Steps** tab.
4. On the Procedure Variables tab, add a procedure variable called `destination_path`.
5. Select the Default Phase, and click **Insert** to add a new step to the phase. On the Create wizard select Type as **Library:Component**. The page refreshes, and a five-step wizard appears.
 - a. On the Create page, enter a unique name **Transfer JRE**, and then click **Next**.
 - b. On the Select Component page, select the Component `hotspot_jre6_linux32`.
 - c. On the Select Directive page, select the directive `install_jre6_linux32`.
 - d. On the Map Properties page, map the directive properties with the variables defined. For example, set the `destination_path` directive property to Choose Variable, and then choose the procedure variable that you set `destination_path`.
 - e. On the review page, review the details, and click **Finish**.
6. Select the step **Transfer JRE**, and click **Insert**. On the Create Wizard, select Type **Host Command**. The page refreshes, and a three-step wizard appears.
 - a. On the Create page, enter a unique name **Check JRE Version**, and then click **Next**.
 - b. On the Enter Command page, enter the following command:


```

          ${data.destination_path}/jre1.6.0_23/bin/java -version
          
```
 - c. On the review page, review the details, and click **Finish**.
7. Go back to the Procedure Library page, and select the **UDDPTest** procedure that you just created, and click **Launch**. To complete the wizard enter the following

details: target where you want to provision your procedure, variable (destination path: /tmp), credential info, and notification information.

8. Once you have provided all the details, click Submit. Enter the a unique Submission name **FirstUDDP**.
9. After the procedure has run, verify the output of the **Check JRE Version** step. Ideally the version should be JRE6.

A.6.3.3 Using EM CLI commands to Run an Instance of the Procedure

Use EM CLI commands to submit the procedure instance:

1. Run the following command to retrieve a list of all the procedures that you have submitted, and note down the instance ID:

```
emcli get_instances
For example: emcli get_instances -type=DemoNG
```

2. Run the following command to get a list of inputs submitted for your procedure:

```
emcli get_instance_data - instance=<procedure_instance_ID>
For example: emcli get_instance_data -instance=16B15CB29C3F9E6CE040578C96093F61
> mydp.properties
```

3. Edit the file (mydp.properties), and change the values of the property destination path to /scratch.
4. Submit the procedure with the modified properties file as the input:

```
emcli submit_procedure -input_file=data:<input_file> -name=<procedure_name>
-procedure=<procedure_guid>
For example: emcli submit_procedure -input_file=data:mydp.properties
-name=UDDPTest -procedure=16B15CB29C3F9E6CE040578C96093F61
```

A.6.4 Patching WebLogic Server Target

This procedure describes how to create a patch plan, update the values in them, and submit them to deploy patches on the selected targets. This workflow captures end-to-end steps on patching WLS targets. The process of patching is the same irrespective of the targets selected.

To patch WebLogic Server targets, follow these steps:

1. Run the following command to search for the release ID of the Oracle WebLogic Release 10.3.5:

```
emcli list_aru_releases -name="10.3.5"
Output:
Release ID      Release Name      Long Release Name
8191035020     10.3.5.0.2       WLS 10.3.5.0.2
8191035010     10.3.5.0.1       WLS 10.3.5.0.1
8191035000    10.3.5          WLS 10.3.5
95103500       10.3.5           WLS 10.3.5
```

2. Run the following command to search for the produc ID of Oracle WebLogic:

```
emcli list_aru_products -name="Oracle WebLogic Server"
Output:
Product ID      Product Name
15991         Oracle WebLogic Server
16725          Oracle WebLogic Server Virtual Edition
```

3. Run the following command to search for the platform ID of a Generic Platform:

```
emcli list_aru_platform -name="Generic Platform"
Output:
Platform ID      Platform Name
2000           Generic Platform
1204             NLS Generic Platform
```

4. Search for the Patch ID using the product, release, and platform details that you have from the previous steps as followings:

```
emcli search_patches -product=15991 -release=8191035000 -platform=2000

Output:
9561331  Generic PLATFORM - 10.3.5 Oracle WebLogic Server 10.3.5  Generic
American English      Recommended      Generic Platform
```

5. Create a patch-target map (properties) file using the *vi* editor, and supply information like Patch ID, Release ID, and Platform ID, Language ID, and so on. Here is a sample properties file:

```
vi create.props

patch.0.patch_id=9561331
patch.0.release_id=8191035000
patch.0.platform_id=2000
patch.0.language_id=0
patch.0.target_name=/Farm01_soa_domain/soa_domain
patch.0.target_type=weblogic_domain
```

6. Run the following command to create the plan, and supply the newly created properties file (create.props) as input:

```
emcli create_patch_plan -name=demo1 -input_file=data:create.props

Output:
The Patch Plan "demo1" is successfully created.
```

7. To view the user-editable fields of an existing plan, and save the output to a properties file run the following command:

```
emcli get_patch_plan_data -name=demo1 >set.props

vi set.props
Output:
name=demo1
description=
deployment_date=
planPrivilegeList=VIEWER:ADMIN:VIEW;OPER:ADMIN:VIEW;DESIGNER:ADMIN:VIEW

patch.0.patch_id=9561331
patch.0.release_id=8191035000
patch.0.platform_id=2000
patch.0.language_id=0
patch.0.target_name=/Farm01_soa_domain/soa_domain
patch.0.target_type=weblogic_domain

deploymentOptions.StageLocation=%emd_emstagedir%
deploymentOptions.AdvancedOPatchOptions=AllNodes
deploymentOptions.StagePatches=true
deploymentOptions.rollbackMode=false
```

8. Edit the properties file (`set.props`) using any editor to change the rollback mode to true:

```
name=demo1
description=
deployment_date=
planPrivilegeList=VIEWER:ADMIN:VIEW;OPER:ADMIN:VIEW;DESIGNER:ADMIN:VIEW

patch.0.patch_id=9561331
patch.0.release_id=8191035000
patch.0.platform_id=2000
patch.0.language_id=0
patch.0.target_name=/Farm01_soa_domain/soa_domain
patch.0.target_type=weblogic_domain

deploymentOptions.StageLocation=%emd_emstagedir%
deploymentOptions.AdvancedOPatchOptions=AllNodes
deploymentOptions.StagePatches=true
deploymentOptions.rollbackMode=true
```

9. To save the patch plan with the new edited data, run the following command:

```
emcli set_patch_plan_data -name=demo1 -input_file=data:set.props
```

Output:

It is successfully updating deployment options from the patch plan.

10. To verify the status of the patch plan, run the following EM CLI command:

```
emcli show_patch_plan -name=demo1 -info
```

Output:

```
<plan>
  <planDetails>
    <plan_id>EDD74FFF006DD0EE6D28394B8AAE</plan_id>
    <name>demo1</name>
    <type>PATCH</type>
    <description/>
    <conflict_check_date>Tue Feb 21 18:04:04 PST 2012</conflict_check_date>
    <conflict_check_date_ms>1329876244000</conflict_check_date_ms>
    <is_deployable>1</is_deployable>
    <plan_status>CONFLICTS</plan_status>
    <review_status>CONFLICT_FREE</review_status>
    <created_date>Tue Feb 21 17:40:47 PST 2012</created_date>
    <created_date_ms>1329874847000</created_date_ms>
    <created_by>SYSMAN</created_by>
    <last_updated_date>Tue Feb 21 17:58:29 PST 2012</last_updated_date>
    <last_updated_date_ms>1329875909000</last_updated_date_ms>
    <last_updated_by>SYSMAN</last_updated_by>
    <grant_priv>yes</grant_priv>
    <user_plan_privilege>FULL</user_plan_privilege>
    <see_all_targets>N</see_all_targets>
    <homogeneousGroupLabel>Oracle WebLogic Domain 10.3.5.0 (Linux
x86-64)</homogeneousGroupLabel>
    <executeGuid/>
    <executeUrl/>
  </planDetails/>
```

11. After you have created and updated the patch plan with all the relevant data, you can submit your patch plan in the following sequence of modes. The EM CLI command used to submit the patch plan is:

```
emcli submit_patch_plan -name=demo1 -action=analyze
```

Output:

The action "analyze" is successfully submitted on the Patch Plan "demo1", now "analyze" is in progress.

- 12.** To verify the status of the patch plan submitted, run the following EM CLI command:

```
emcli show_patch_plan -name=demo1 -info
```

Output:

```
<plan>
  <planDetails>
    <plan_id>EDD74FFF006DD0EE6D28394B8AAE</plan_id>
    <name>demo1</name>
    <type>PATCH</type>
    <description/>
    <conflict_check_date>Tue Feb 21 18:04:04 PST 2012</conflict_check_date>
    <conflict_check_date_ms>1329876244000</conflict_check_date_ms>
    <is_deployable>1</is_deployable>
    <plan_status>CONFLICTS</plan_status>
    <review_status>CONFLICT_FREE</review_status>
    <created_date>Tue Feb 21 17:40:47 PST 2012</created_date>
    <created_date_ms>1329874847000</created_date_ms>
    <created_by>SYSMAN</created_by>
    <last_updated_date>Tue Feb 21 17:58:29 PST 2012</last_updated_date>
    <last_updated_date_ms>1329875909000</last_updated_date_ms>
    <last_updated_by>SYSMAN</last_updated_by>
    <grant_priv>yes</grant_priv>
    <user_plan_privilege>FULL</user_plan_privilege>
    <see_all_targets>N</see_all_targets>
    <homogeneousGroupLabel>Oracle WebLogic Domain 10.3.5.0 (Linux
x86-64)</homogeneousGroupLabel>
    <executeGuid/>
    <executeUrl/>
  </planDetails/>
```

- 13.** To check if there are any conflicts, run the following command:

```
emcli show_patch_plan -name=planName -analysisResults
```

Output:

```
<plan_status>CONFLICTS</plan_status>
```

You can verify the plan you have created by logging in to Enterprise Manager Cloud Control, from **Enterprise** menu, select **Provisioning and Patching**, then select **Patches and Updates**. On the home page, you will see the patch plan **demo1** that you have created using the command line as follows:

<input type="checkbox"/>	agent	Review Analysis	Patch	Not Specified	SYSMAN
<input type="checkbox"/>	demo	Review Analysis	Patch	Not Specified	SYSMAN
<input type="checkbox"/>	demo1	Review Analysis	Patch	Not Specified	SYSMAN
<input type="checkbox"/>	hh	Review Analysis	Patch	Not Specified	SYSMAN
<input type="checkbox"/>	ss	Review Analysis	Patch	Not Specified	SYSMAN
<input type="checkbox"/>	wls4	Successfully Analyzed	Patch	Not Specified	SYSMAN
<input type="checkbox"/>	wls	Deployed Successfully	Patch	Not Specified	SYSMAN

You can resolve the conflicts using the UI, and then submit the patch plan.

14. Run the command `show_patch_plan` after resolving the conflicts to verify the status of the plan as follows:

```
Output:
<plan>
  <planDetails>
    <plan_id>EDD74FFF006DD0EE6D28394B8AAE</plan_id>
    <name>demo</name>
    <type>PATCH</type>
    <description/>
    <conflict_check_date>Tue Feb 21 18:04:04 PST 2012</conflict_check_date>
    <conflict_check_date_ms>1329876244000</conflict_check_date_ms>
    <is_deployable>1</is_deployable>
    <plan_status>INPROGRESS</plan_status>
    <review_status>CONFLICT_FREE</review_status>
    <created_date>Tue Feb 21 17:40:47 PST 2012</created_date>
    <created_date_ms>1329874847000</created_date_ms>
    <created_by>SYSMAN</created_by>
    <last_updated_date>Tue Feb 21 17:58:29 PST 2012</last_updated_date>
    <last_updated_date_ms>1329875909000</last_updated_date_ms>
    <last_updated_by>SYSMAN</last_updated_by>
    <grant_priv>yes</grant_priv>
    <user_plan_privilege>FULL</user_plan_privilege>
    <see_all_targets>N</see_all_targets>
    <homogeneousGroupLabel>Oracle WebLogic Domain 10.3.5.0 (Linux
x86-64)</homogeneousGroupLabel>
    <executeGuid>BA8E3904DDB36CFE040F00A5E644D13</executeGuid>
    <executeUrl>/em/console/paf/procedureStatus?executionGUID=BA8E3904DDB36CFE040F
00A5E644D13</executeUrl>
  </planDetails/>
```

15. Run the following command to determine the status of the patch plan execution:

```
emcli get_instance_status -instance=BA8E3904DDB36CFE040F00A5E644D13
```

```
Output:
BA8E3904DDB36CFE040F00A5E644D13, PatchOracleSoftware, demo1_Analysis_Tue Mar
06 02:08:02 PST 012, EXECUTING
```

16. After a successful analysis, you can deploy/prepare the patch plan. To do so, run the following command with action **deploy**:

```
emcli submit_patch_plan -name=demo1 -action=deploy
```

```
Output:
The action "deploy" is successfully submitted on the Patch Plan "demo1", now
"deploy" is in progress
```

17. Use the Cloud Control UI to see if the submitted plan has successfully been deployed. Alternately, you can verify the same using the EM CLI command:

```
emcli get_job_execution_detail -execution=79CAF6A6DAFCFEE6654C425632F19411 -xml
```

A.6.5 Creating a New Generic Component by Associating a Zip File

To upload a zip file as a new component, follow these steps:

- [Step 1: Identifying the Parent Folder in Software Library](#)
- [Step 2: Creating a Genetic Component Entity](#)
- [Step 3: Associating a Zip File to the Generic Component](#)

- [Step 4: Verifying the Newly Created Entity](#)

A.6.5.1 Step 1: Identifying the Parent Folder in Software Library

Any new entity created in Software Library must be placed in a folder. You can either choose an existing folder, or create a new one. To do so, follow these sections:

- [Creating a New Folder](#)
- [Choosing an Existing Folder](#)

Creating a New Folder

To create a new folder, the parent folder should be identified. If the parent folder is the **root** folder (displayed as the top level "Software Library" folder), then use the following EM CLI verb:

```
emcli create_swlib_folder
-name="myFolder"
-desc="myFolder description"
-parent_id=ROOT
```

Output:

Folder myFolder is created in Software Library folder, identifier is oracle:defaultService:em:provisioning:1:cat:C771B5A38A484CE3E40E50AD38A69D2.

You can use the identifier of the newly created folder that is part of the output message when creating or modifying entities, or for creating other sub-folders.

Choosing an Existing Folder

To choose an existing folder, you can use either of the following approaches:

- [Approach 1: Using Enterprise Manager UI](#)
- [Approach 2: Using Enterprise Manager Command Line Interface](#)

Approach 1: Using Enterprise Manager UI

Follow these steps:

1. From the **Enterprise** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library home page, from **View** menu select **Columns**, and then select **Internal ID**. By default, the Internal ID column is hidden.
3. Copy the Internal ID column value of the folder you want.

Approach 2: Using Enterprise Manager Command Line Interface

Use the following EM CLI verb:

```
emcli list_swlib_folders
-parent_id=ROOT
-show_folder_id
```

Output:

```
Java EE Provisioning,Java EE Application Provisioning
Entities,oracle:defaultService:em:provisioning:1:cat:C771B5AAF4A4EED9E040E
50AD38A6E98
```

```
MultiOMS,List of Oracle shipped
Directives,oracle:defaultService:em:provisioning:1:cat:C771B5AAF1ACEED9E04
0E50AD38A6E98

myFolder,myFolder
description,oracle:defaultService:em:provisioning:1:cat:C771B5A38A484CE3E0
40E50AD38A69D2

OSBProvisioning,OSBProvisioning
Entities,oracle:defaultService:em:provisioning:1:cat:C771B5AAF3F1EED9E040E
50AD38A6E98

.....
```

If the folder you want to access is a sub-folder of myFolder, then use the following verb to list the sub-folders by specifying the identifier of myFolder, as follows:

```
emcli list_swlib_folders
-parent_
id='oracle:defaultService:em:provisioning:1:cat:C771B5A38A484CE3E040E50AD38A69D2'
-show_folder_id
```

Output:

```
mySubFolder,mySubFolder
description,oracle:defaultService:em:provisioning:1:cat:C771B5A38A494CE3E0
40E50AD38A69D2
```

A.6.5.2 Step 2: Creating a Genetic Component Entity

To create an entity of type Component and subtype Generic Component under mySubFolder folder, follow these sections:

- [Step 1a. Identifying the Entity Type](#)
- [Step 1b. Identifying the Entity Subtype](#)
- [Step 2. Creating a Generic Component Entity](#)

Step 1a. Identifying the Entity Type

To list all the available types in Software Library, use the following verb:

```
emcli list_swlib_entity_types
-show_type_id
```

Output:

```
Component, COMP_Component
Directives, COMP_Directives
Bare Metal Provisioning, BMPType
Virtualization, Virtualization
```

Step 1b. Identifying the Entity Subtype

To list all the subtypes for the component type, use the following verb:

```
emcli list_swlib_entity_subtypes
-entity_type_id=COMP_Component
-show_subtype_id
```

Output:

```
Generic Component, SUB_Generic
Oracle Database Software Clone, SUB_OracleDB
```

```

Configuration Template, SUB_ConfigTpl
Oracle Application Server, SUB_OracleAS
Self Update, SUB_SelfUpdate
Oracle Clusterware Clone, SUB_OracleCRS
OSB Resource, SUB_OSBResource
Oracle Software Update, SUB_OraSoftUpdate
Java EE Application, SUB_JavaEEApplication
Installation Media, SUB_InstallationMedia
Database Template, SUB_DbCreateTemplate
Database Provisioning Profile, SUB_DbProfile
WebLogic Domain Provisioning Profile, SUB_FMWBundle
WebLogic Domain Clone, SUB_WLSTemplate
Oracle Middleware Home Gold Image, SUB_FMWImage

```

Step 2. Creating a Generic Component Entity

To create a generic component, run the following verb:

```

emcli create_swlib_entity
-name=myEntity
-type=COMP_Component
-subtype=SUB_Generic
-folder_
id='oracle:defaultService:em:provisioning:1:cat:C771B5A38A494CE3E040E50AD38A69D2'
-desc='myEntity description'
-attr="PRODUCT:Example"
-attr="PRODUCT_VERSION:3.1"
-attr="VENDOR:Example Corp"
-note='first comment for myEntity

```

Note: The type and subtype options are optional when creating a Generic Component, but has been used explicitly for this illustration.

Output:

```

Entity 'myEntity' is created in 'mySubFolder' folder, identifier is
'oracle:defaultService:em:provisioning:1:cmp:COMP_Component:SUB_
Generic:C77200CA9DC1E7AAE040E50AD38A1599:0.1'

```

Note: You can use the identifier of the newly created entity that is part of the output message when uploading files or modifying the entity.

To verify the newly created entity, use the following verb:

```

emcli list_swlib_entities
-name=myEntity
-folder_
id='oracle:defaultService:em:provisioning:1:cat:C771B5A38A494CE3E04
0E50AD38A69D2'

```

Output:

```

myEntity,0.1,myEntity description,Ready,Component,Generic
Component,Untested,SYSMAN

```

A.6.5.3 Step 3: Associating a Zip File to the Generic Component

To upload a zip file to an existing entity `myEntity`, use the following verb:

```
emcli upload_swlib_entity_files
-entity_rev_id='oracle:defaultService:em:provisioning:1:cmp:COMP_Component:SUB_
Generic:C77200CA9DC1E7AAE040E50AD38A1599:0.1'
-file="/scratch/user1/patch13653908.zip;newfile1.zip"
-host="adc2190533.us.example.com"
-credential_name=mycred11
-credential_owner=sysman
```

Note: A new revision of the entity `myEntity` will be created after the upload is complete.

Output:

```
Upload of file(s) initiated, this may take some time to complete...
Upload of file(s) completed successfully.
Entity 'myEntity (0.2)' in 'mySubFolder' folder has been created, identifier is
'oracle:defaultService:em:provisioning:1:cmp:COMP_Component:SUB_
Generic:C77200CA9DC1E7AAE040E50AD38A1599:0.2'.
```

Alternately, to refer to a zip file present in an **HTTP** reference location, say `myScripts`, use the following verb:

```
emcli refer_swlib_entity_files
-entity_rev_id='oracle:defaultService:em:provisioning:1:cmp:COMP_Component:SUB_
Generic:C77200CA9DC1E7AAE040E50AD38A1599:0.1'
-file='scripts/perl/script1.pl;new_script.pl'
-refer_storage='myScripts;Http'
```

Output:

```
Entity 'myEntity (0.2)' in 'mySubFolder' folder has been created, identifier is
'oracle:defaultService:em:provisioning:1:cmp:COMP_Component:SUB_
Generic:C77200CA9DC1E7AAE040E50AD38A1599:0.2'.
```

A.6.5.4 Step 4: Verifying the Newly Created Entity

To verify the newly created entity, use the following verb:

```
emcli list_swlib_entities
-name=myEntity
-folder_
id='oracle:defaultService:em:provisioning:1:cat:C771B5A38A494CE3E040E50AD38A69D2'
```

Output:

```
myEntity,0.1,myEntity description,Ready,Component,Generic
Component,Untested,SYSMAN
```

A.7 Limitations of Using Enterprise Manager Command Line Interface

Following are the limitations of using EM CLI for running the deployment procedures:

- You cannot add or edit steps and phases using EM CLI commands. To do so, you must log in to Cloud Control, and follow the steps described in the section [Section 33.2.1](#).

- You cannot define new variables to be used in the deployment procedures through EM CLI, this can be done only through the Cloud Control UI. For more information about procedure variables, see [Section 32.3.2](#).
- You cannot track the detailed execution info (such as failures) of an instance through EM CLI, which is possible through the Cloud Control UI.
- To set the *My Oracle Support* preferred credentials, you must log in to the Enterprise Manager Cloud Control. There is no command line option to do so.
- Patches can be uploaded to Software Library only through Cloud Control, you can not do the same using the EM CLI.

Checking Host Readiness

This appendix describes the settings you must make on the hosts before you can use them for provisioning and patching tasks. In particular, this appendix covers the following:

- [Setting Up User Accounts](#)
- [Shell Limits](#)
- [Root Setup \(Privilege Delegation\)](#)
- [Environment Settings](#)
- [Storage Requirements](#)
- [Installation Directories and Oracle Inventory](#)

B.1 Setting Up User Accounts

To use a host for provisioning a database, you must ensure that groups such as `oinstall`, `dba`, `oper`, and `asmadmin` are set up. Also, the user running these provisioning tasks must be added to these groups. To create the following groups, and ensure that the host user is part of these groups, you can run the following commands:

- To create the database groups:
 - `groupadd oinstall`
 - `groupadd dba`
 - `groupadd oper`
 - `groupadd asmadmin`
- To add a host user to these groups, run the following command, and enter the password when prompted.

```
useradd -u 500 -g oinstall -G dba,oper,asmdba oracle
```

Where,

-u option specifies the user ID.

-g option specifies the primary group, which must be the Oracle Inventory group, for example `oinstall`.

-G option specifies the secondary groups, which must include the OSDBA group, and, if required, the OSOPER and ASMDBA groups, for example, `dba`, `asmdba`, or `oper`.

B.1.1 Configuring SSH

In case of a clustered environment, to configure SSH on each node in a cluster, you must log in as an Oracle user, and run the following commands on every node:

```
su - oracle
mkdir ~/.ssh
chmod 700 ~/.ssh
/usr/bin/ssh-keygen -t rsa # Accept the default settings
```

B.2 Shell Limits

To improve the performance of the software on Linux systems, increase the following shell limits for the Oracle software owner users such as `crs`, `oracle`, `asm`, and so on. To do so, run the following commands:

- Add the following values into the `limits.conf` file located under the `/etc/security/` directory:
 - oracle soft nproc 2047
 - oracle hard nproc 16384
 - oracle soft nofile 1024
 - oracle hard nofile 65536
- Add the following line into the `/etc/pam.d/login` file, or edit the `/etc/pam.d/login` file to include the following if it does not exist already:
`session required pam_limits.so`

B.3 Root Setup (Privilege Delegation)

Provisioning Applications require some of the scripts to be run as a super user. To do so, you must ensure that host user has `root` privileges. To authorize other users' root privileges, you can use the authentication utilities such as SUDO, PowerBroker, and so on. This support is offered in Cloud Control using the Privilege Delegation mechanism. Technically, Privilege Delegation is a framework that allows you to use either SUDO or PowerBroker to perform an activity with the privileges of another user (locked accounts).

For more information about configuring Privilege Delegation Settings, see [Section 2.3.3](#).

B.4 Environment Settings

Meet the following recommended host settings before proceeding with the provisioning tasks:

- [Kernel Requirements](#)
- [Node Time Requirements](#)
- [Package Requirements](#)
- [Memory and Disk Space Requirements](#)
- [Network & IP Address Requirements](#)

Note: For details about all the recommended parameters, refer the following link:
<http://www.oracle.com/technetwork/topics/linux/validated-configurations-085828.html>

B.4.1 Kernel Requirements

Enter the commands displayed in the following table to view the current values of the kernel parameters. Make a note of the current values and identify any values that you must change. To change any of the existing values, you will have to add or edit the variable values in the `/etc/sysctl.conf` file.

Note: To change the current kernel parameters, run the following command with root user privileges:

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

Parameter	Command
semmsl, semmns, semopm, and semmni	# /sbin/sysctl -a grep sem This command displays the value of the semaphore parameters in the order listed.
shmall, shmmax, and shmmni	# /sbin/sysctl -a grep shm This command displays the details of the shared memory segment sizes.
file-max	# /sbin/sysctl -a grep file-max This command displays the maximum number of file handles.
ip_local_port_range	# /sbin/sysctl -a grep ip_local_port_range This command displays a range of port numbers.
rmem_default	# /sbin/sysctl -a grep rmem_default
rmem_max	# /sbin/sysctl -a grep rmem_max
wmem_default	# /sbin/sysctl -a grep wmem_default
wmem_max	# /sbin/sysctl -a grep wmem_max

Note: For more information about the Kernel requirements, see the *Oracle Database Installation Guide* available in the following location:
http://www.oracle.com/pls/db112/portal.portal_db?selected=11&frame=#linux_installation_guides

B.4.2 Node Time Requirements

In case of a clustered environment, ensure that each member node of the cluster is set as closely as possible to the same date and time. To do so, Oracle recommends using the Network Time Protocol (NTP) feature available in your operating systems, with all nodes using the same reference Network Time Protocol server.

For Oracle Cluster Time Synchronization Service (ctssd) to synchronize the times of the Oracle RAC nodes, NTP must be configured. If you are using NTP, then do the following:

1. Add the `-x` option to the `/etc/sysconfig/ntpd` file, and restart `ntpd` as follows:

```
OPTIONS="-x -u ntp:ntp -p /var/run/ntpd.pid"
```
2. Restart Network Time Protocol server:

```
# service ntpd restart
```
3. Check the configuration level as follows:

```
chkconfig --level 35 nscd on
```
4. Start the Name Service Cache Daemon (`nscd`):

```
service nscd start
```

B.4.3 Package Requirements

Run the following command as a root user to ensure that you have the required packages installed:

```
rpm -q binutils elfutils-libelf elfutils-libelf-devel glibc glibc-common
glibc-devel gcc gcc-c++ libaio libaio-devel libstdc++ libstdc++-devel make
compat-libstdc++ sysstat unixODBC unixODBC-devel iscsi-initiator-utils
libgcc
```

If the packages are not installed, then refer the following link to download and install the required packages:

<http://www.oracle.com/technetwork/topics/linux/validated-configurations-085828.html>

B.4.4 Memory and Disk Space Requirements

Ensure that the host meets the following memory requirements:

1. A minimum of least 1 GB of physical RAM should be available. To determine the current physical RAM size on your host, run the following command:

```
grep MemTotal /proc/meminfo
```
2. The following table describes the relationship between the installed RAM and the configured swap space recommendation:

Available RAM	Swap Space Requirements
Between 1 GB and 2 GB	1.5 times the size of RAM
Between 2 GB and 8 GB	Equal to the size of RAM
More than 8 GB	0.75 times the size of RAM

3. To determine the amount of disk space available in the `/tmp` directory, run the following command:

```
df -kh /tmp
```

B.4.5 Network & IP Address Requirements

In case of a clustered environment, ensure that each node has at least two network adapters or network interface cards (NICs). One for the public network interface, and the other for the private network interface (the interconnect)

Following are the network configuration requirements:

Public Network Interface	Private Network Interface
The public interface names associated with the network adapters for each network must be the same on all nodes.	The private interface names associated with the network adapters should be the same on all nodes.
Each network adapter must support TCP/IP	The interconnect must support the user datagram protocol (UDP) using high-speed network adapters and switches that support TCP/IP (Gigabit Ethernet or better required).
	Note: For the private network, the endpoints of all designated interconnect interfaces must be completely reachable on the network. There should be no node that is not connected to every private network interface. You can test whether an interconnect interface is reachable using a ping command.

Before starting the installation, you must have the following IP addresses available for each node:

1. An IP address with an associated host name (or network name) registered in the DNS for the public interface. If you do not have an available DNS, then record the host name and IP address in the system hosts file, `/etc/hosts`.
2. One virtual IP (VIP) address with an associated host name registered in a DNS. If you do not have an available DNS, then record the host name and VIP address in the system hosts file, `/etc/hosts`.
3. A private IP address with a host name for each private interface.

For example, for a two node cluster where each node has one public and one private interface, you might have the configuration shown in the following table for your network interfaces, where the hosts file is `/etc/hosts`:

Node	Host Name	Type	IP Address	Registered In
node1	node1	Public	143.46.43.100	DNS (if available, else the hosts file)
node1	node1-vip	Virtual	143.46.43.104	DNS (if available, else the hosts file)
node1	node1-priv	Private	10.0.0.1	Hosts file
node2	node2	Public	143.46.43.101	DNS (if available, else the hosts file)
node2	node2-vip	Virtual	143.46.43.105	DNS (if available, else the hosts file)
node2	node2-priv	Private	10.0.0.2	Hosts file

To enable VIP failover, the configuration shown in the preceding table defines the public and VIP addresses of both nodes on the same subnet, `143.46.43`.

B.5 Storage Requirements

There are two ways of storing Oracle Clusterware files:

- Oracle Automatic Storage Management (Oracle ASM): You can install Oracle Clusterware files (Oracle Cluster Registry and voting disk files) in Oracle ASM disk groups.
- A supported shared file system: Supported file systems include the NFS & OCFS.

The following table describes the various storage options for Oracle Clusterware and Oracle RAC:

Storage Option	OCR and Voting Disk Files	Oracle Clusterware binaries	Oracle RAC binaries	Oracle Database Files
Oracle Automatic Storage Management (Oracle ASM)	Yes	No	No	Yes
Note: Loopback devices are not supported for use with Oracle ASM				
Oracle Automatic Storage Management Cluster File System (Oracle ACFS)	No	No	Yes	No
Local file system	No	Yes	Yes	No
NFS file system on a certified NAS filer	Yes	Yes	Yes	Yes
Note: Direct NFS does not support Oracle Clusterware files.				
Shared disk partitions (block devices or raw devices)	Not supported by OUI or ASMCA, but supported by the software. They can be added or removed after installation.	No	No	Not supported by OUI or ASMCA, but supported by the software. They can be added or removed after installation.

The following table displays the File System Volume Size requirements:

Oracle Clusterware Shared File System Volume Size Requirements

File Types Stored	Number of Volumes	Volume Size
Voting disks with external redundancy	3	At least 300 MB for each voting disk vol
Oracle Cluster Registry (OCR) with external redundancy	1	At least 300 MB for each OCR volume
Oracle Clusterware files (OCR and voting disks) with redundancy provided by Oracle software.	1	At least 300 MB for each OCR volume At least 300 MB for each voting disk vol

Oracle RAC Shared File System Volume Size Requirements

File Types Stored	Number of Volumes	Volume Size
Oracle Database files	1	At least 1.5 GB for each volume
Recovery files	1	At least 2 GB for each volume

Note: Recovery files must be on a different volume than database files

B.6 Installation Directories and Oracle Inventory

Ensure that the installation directories where you plan to provision the Oracle Products are clean. As per Optimal Flexible Architecture (OFA) standards, Oracle base directory should be available in the following path:

```
/mount_point/app/oracle_sw_owner
```

Where, `mount_point` is the mount point directory for the file system that will contain the Oracle software.

Note: Ensure that the user performing the installation has write access on the mount points. To verify that the user has the required permissions, run the following command:

```
chown -R oracle:oinstall <mount point>
```

For example:

If the permission is denied while mounting:

```
[root@node2-pub ~]# mkdir -p /u01/app/test
```

```
[root@node2-pub ~]# permission denied
```

To resolve the permission issue, run the following command:

```
[root@node2-pub root]# chown -R oracle:oinstall /u01
```

Using emctl partool Utility

This appendix introduces you to the emctl partool utility and explains how you can use it to perform critical tasks such as exporting Deployment Procedures as PAR files, importing PAR files, and so on. In particular, this appendix covers the following:

- [Overview of Provisioning Archive Files](#)
- [Overview of emctl partool Utility](#)
- [Checking Oracle Software Library](#)
- [Exporting Deployment Procedures](#)
- [Importing PAR Files](#)

Note: Provisioning Archive Files that were exported from any Enterprise Manager version prior to 12c can not be imported into Enterprise Manager 12c.

C.1 Overview of Provisioning Archive Files

Provisioning Archive (PAR) files are archive files that contain a collection, or bundle of Deployment Procedures and Software Library entities that are used in numerous Lifecycle Management tasks like Provisioning and Patching applications.

In case of a Deployment Procedures, partool exports only the User-defined procedures, and not the Oracle-owned procedures. While exporting the User-defined procedure, the complete deployment procedure is not exported, only the customization (delta changes) are exported.

Also, note that in case of upgrade all the procedures that were created pre-12c can not be exported using the partool export utility.

Note: For importing PAR files that contain Software Library entities, ensure that your Software Library is configured. For information on Configuring Software Library, see *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

C.2 Overview of emctl partool Utility

Over a period of time, you might have customized some Deployment Procedures, and you might want to reuse them in another instance of Cloud Control. Under such circumstances, you might want to export the customized Deployment Procedures

from one instance of Cloud Control, and deploy them to another instance of Cloud Control.

emctl partool utility is a tool offered by Cloud Control that helps you perform these functions using the command line interface. Essentially, emctl partool utility helps you:

- Export Deployment Procedures and its associated components and directives as PAR files
- Import PAR files to the same instance or any other instance of Cloud Control

The emctl partool utility is located in the \$ORACLE_HOME/bin directory.

The following is the usage information displayed when you run \$ORACLE_HOME/bin/emctl partool:

```
emctl partool <deploy|view> -parFile <file> -force(optional)
emctl partool <deploy|view> -parFile <file> -force(optional) -ssPasswd <password>
emctl partool <deploy|view> -parDir <dir> -force(optional)
emctl partool export -guid <procedure guid> -file <file> -displayName <name>
  -description <desc> -metadataOnly(optional)
emctl partool check
emctl partool help
```

Table C–1 describes the additional options that can be used with the emctl partool utility.

Table C–1 *emctl partool Options*

Option	Description
-repPasswd <repPassword>	Indicates the repository password. User will be prompted for the repository password if -repPasswd is not specified on the command line. Note: Providing a password on the command line is insecure and should be avoided in a production environment.
-force	Forces the Software Library entities to be created or uploaded again. If already present, it creates a new revision.
check	Checks whether the Software Library is configured.
-file <file>	Represents the PAR file.
-action <deploy view export>	Deploys, views, or exports PAR files.
-verbose	Indicates verbose mode.
help	Displays Help information.
-displayName <displayName>	Indicates PAR file name.
-parDir <dir>	Directory where the PAR files are located.
-metadataOnly	Flag for metadata-only exports.
-guid <guid>	Procedure GUID to export. To export multiple procedures, provide the GUIDs separated by ","
-parFile <file>	Path to the PAR file.
-description <description>	PAR file description.

Table C-1 (Cont.) emctl partool Options

Option	Description
-ssPasswd <secretStorePassword>	<p>This is optional.</p> <p>If used with -action export; if any of the exported Software Library entity contains a secret property, an Oracle Wallet is created to store the value of the secret property. Oracle Wallet is created using the specified password. You are prompted to enter a password if -ssPasswd switch is used and if password is not supplied as a command line argument. You must use the same password while importing the PAR file in a new repository.</p> <p>If used with -action <deploy view>; if the PAR file contains any password protected Oracle Wallet (that stores an entity's secret property values), then this parameter is required to open the store. You are prompted to enter a password if -ssPasswd switch is used and password is not specified as a command line argument.</p>

C.3 Checking Oracle Software Library

Before running the emctl partool utility to export or import PAR files, ensure that the \$ORACLE_HOME environment variable is set to the Oracle home directory of Oracle Management Service (OMS) and a Software Library path is configured.

To check the Software Library, run the following command:

```
$ORACLE_HOME/bin/emctl partool check
```

C.4 Exporting Deployment Procedures

To export Deployment Procedures, you must first obtain the GUID of those Deployment Procedures, and then run the emctl partool utility to create a PAR file. This section explains the following:

- [Obtaining Deployment Procedure's GUID](#)
- [Creating PAR File](#)

C.4.1 Obtaining Deployment Procedure's GUID

To obtain the GUID of a Deployment Procedure using Cloud Control, follow these steps:

1. In Cloud Control, from the **Enterprise** menu select **Provisioning and Patching**, and then click **Procedure Library**.
2. On the Provisioning page, right click the deployment procedure name and from the menu select **Copy Link Location**.
3. Paste the copy the link to a notepad, and then search for **guid**.

For example:

```
https://adc2171248.us.example.com:14500/em/console/paf/procedureView?guid=B3B4B6C76AE46A67E040E50A65751782
```

The GUID is B3B4B6C76AE46A67E040E50A65751782

Alternately you can use the following EMCLI command to retrieve the GUID of the procedure:

```
emcli get_procedures [-type={procedure type}] [-parent_proc={procedure associate  
with procedure configuration}]
```

Example:

```
emcli get_procedures -type=DemoNG -parent_proc=ComputeStepTest
```

Output Column:

GUID, Procedure type, name, display name, version, Parent procedure name

Note: For more information about setting EMCLI, see *Oracle Enterprise Manager Command Line Interface*

C.4.2 Creating PAR File

To create a PAR file that contains one or more Deployment Procedures, run the emctl partool utility with the *export* option as the *action*, and quote the GUIDs of the Deployment Procedures you want to export. Ensure that you separate the GUIDs by a comma.

```
$ORACLE_HOME/bin/emctl partool export -guid <GUID> -file exportedDP.par  
-displayName "User exported DP" -description "<description>"
```

For example, if the GUID of the Deployment Procedure that you want to export is FAC05DD31E3791C3E030579D23106C67, then run the following command:

```
$ORACLE_HOME/bin/emctl partool export -guid  
FAC05DD31E3791C3E030579D23106C67 -file exportedDP.par -displayName "User  
exported DP" -description "Deployment Procedure to be copied to other OMS"
```

After you run this command, a new PAR file named exportedDP.par is created in the directory where you ran the command. You can then import this PAR file to the same instance of Cloud Control or another instance, multiple times.

To export multiple deployment procedures, separate the GUIDs with commas as follows:

```
$ORACLE_HOME/bin/emctl partool export -guid  
"06B62B6ED5DA20BCE040578C850862A7,0C96E96D9818BC5FE040578C8508620F,09AEFF3  
31025AAD0EE40578C85FB5772" -file $ENV{T_WORK}/tvmgf_partool_multi_dp.par  
-displayName "partool multi dp test" -description "partool multi dp test  
description" -repPasswd sysman
```

Note: When a procedure is exported using emctl partool, any directives or components referred by the procedure are also exported. However, only the latest revision of these directives or components will be exported. If you do not want to export components or directives, you can specify the *-metadataOnly* flag when running emctl partool.

C.5 Importing PAR Files

You can import PAR files using the command line interface or the graphical user interface offered by Cloud Control, that is, the console. This section explains the following:

- [Importing Using Command Line Interface](#)

- [Importing Using Cloud Control Console](#)

Note: Importing an existing PAR file (from the previous releases) into Enterprise Manager Cloud Control 12c is not supported. For example, you cannot import a Enterprise Manager 11g Grid Control Release 1 (11.1.0.0) to Enterprise Manager Cloud Control 12c.

C.5.1 Importing Using Command Line Interface

This section covers the following:

- [Importing Specific PAR File](#)
- [Importing All PAR Files](#)

C.5.1.1 Importing Specific PAR File

To import or deploy a specific PAR file, run the following command:

```
$ORACLE_HOME/bin/emctl partool deploy -parFile $ORACLE_
HOME/sysman/prov/paf/<par_file_name>
```

For example:

```
$ORACLE_HOME/bin/emctl partool deploy -parFile $ORACLE_
HOME/sysman/prov/paf/asprov.par
```

Note: If Software Library or the procedure already exists in Enterprise Manager and you want to create a new revision of the PAR file, then you can use the `-force` attribute as follows:

```
$ORACLE_HOME/bin/emctl partool deploy -parFile $ORACLE_
HOME/sysman/prov/paf/asprov.par -force
```

Note: If you have multiple OMSes in your environment, then you need run the emctl partool utility only once to deploy any PAR files or to perform other related operations.

While importing PAR files if the user procedure already exists in the setup, then it will always import this procedure with revised (bumped up) version.

C.5.1.2 Importing All PAR Files

To import or deploy all the PAR files in a directory, run the following command:

```
$ORACLE_HOME/bin/emctl partool deploy -parDir $ORACLE_
HOME/sysman/prov/paf/ -force
```

C.5.2 Importing Using Cloud Control Console

To import PAR files or deploy them to an OMS, you can use the emctl partool utility. Alternatively, you can import them from Cloud Control .

For importing the PAR files, follow these steps:

1. In Cloud Control, from the **Enterprise** menu select **Provisioning and Patching**, and then click **Procedure Library**.

2. On the Deployment Procedure Manager page, select the procedure, and from the drop down menu select **Import**, and then click **Go**.
3. On the Upload Procedure File page, select:
 - **Upload from Local Machine** to upload the PAR file from the local machine. Click **Browse** to select the PAR file. Click **Import** to import the file.
 - **Upload from Management Agent Machine** to select the Management Agent target. Enter the Normal or Privileged Host Credential details to access the Management Agent machine where the file is present, and then click **Import** to import the file.

See Also: For a usecase on using the Upload Procedure File feature, see [Section 33.6](#).

Note: When importing or exporting components and/or directives that contain properties with secret values, you must use the `-ssPasswd` command and provide the secret store password to create Oracle Wallet. This ensures that the properties with secret values are securely stored using an Oracle Wallet, and can be accessed while importing with only the Oracle Wallet password.

For more information about the `-ssPasswd` command, see [Table C-1](#).

Understanding PXE Booting and Kickstart Technology

This appendix explains PXE booting and kickstart technology in the following section:

- [About PXE Booting and Kickstart Technology](#)
- [Subnet Provisioning Usecases](#)

D.1 About PXE Booting and Kickstart Technology

One of the key requirements of provisioning is the hardware server's ability to boot over the network instead of a diskette or CD-ROM. There are several ways computers can boot over a network, and Preboot Execution Environment (PXE) is one of them. PXE is an open industry standard supported by a number of hardware and software vendors. PXE is part of the "Wired for Management" (WfM) specification, which is part of a bigger PC98 specification defined by Intel and Microsoft in 1998. A detailed document on PXE specification can be found at <http://www.pix.net/software/pxeboot/archive/pxespec.pdf>.

PXE works with Network Interface Card (NIC) of the system by making it function like a boot device. The PXE-enabled NIC of the client sends out a broadcast request to DHCP server, which returns with the IP address of the client along with the address of the TFTP server, and the location of boot files on the TFTP server. The following steps describe how it works:

1. Target Machine (either bare metal or with boot sector removed) is booted.
2. The Network Interface Card (NIC) of the machine triggers a DHCP request.
3. DHCP server intercepts the request and responds with standard information (IP, subnet mask, gateway, DNS etc.). In addition, it provides information about the location of a TFTP server and boot image (pxelinux.0).
4. When the client receives this information, it contacts the TFTP server for obtaining the boot image.
5. TFTP server sends the boot image (pxelinux.0), and the client executes it.
6. By default, the boot image searches the pxelinux.cfg directory on TFTP server for boot configuration files on the TFTP server using the following approach:

First, it searches for the boot configuration file that is named according to the MAC address represented in lower case hexadecimal digits with dash separators. For example, for the MAC Address "88:99:AA:BB:CC:DD", it searches for the file 01-88-99-aa-bb-cc-dd.

Then, it searches for the configuration file using the IP address (of the machine that is being booted) in upper case hexadecimal digits. For example, for the IP Address "192.0.2.91", it searches for the file "C000025B".

If that file is not found, it removes one hexadecimal digit from the end and tries again. However, if the search is still not successful, it finally looks for a file named "default" (in lower case).

For example, if the boot file name is /tftpboot/pxelinux.0, the Ethernet MAC address is 88:99:AA:BB:CC:DD, and the IP address 192.0.2.91, the boot image looks for file names in the following order:

```
/tftpboot/pxelinux.cfg/01-88-99-aa-bb-cc-dd
/tftpboot/pxelinux.cfg/C000025B
/tftpboot/pxelinux.cfg/C000025
/tftpboot/pxelinux.cfg/C00002
/tftpboot/pxelinux.cfg/C0000
/tftpboot/pxelinux.cfg/C000
/tftpboot/pxelinux.cfg/C00
/tftpboot/pxelinux.cfg/C0
/tftpboot/pxelinux.cfg/C
```

7. The client downloads all the files it needs (kernel and root file system), and then loads them.
8. Target Machine reboots.

The Provisioning application uses Redhat's Kickstart method to automate the installation of Redhat Linux on target machines. Using kickstart, the system administrator can create a single file containing answers to all the questions that will usually be asked during a typical Red Hat Linux installation.

The host specific boot configuration file contains the location of the kickstart file. This kickstart file would have been created earlier by the stage directive of the OS image based on the input from user.

D.2 Subnet Provisioning Usecases

Following are examples of subnet provisioning usecases:

Subnet of size 256

IP Prefix: 192.168.1.0

Subnet Mask: 255.255.255.0

Covers IPs from 192.168.1.0 - 192.168.1.255

Subnet of size 16

IP Prefix: 192.168.1.0

Subnet Mask: 255.255.255.240

Troubleshooting Issues

This appendix provides solutions to common issues you might encounter when using provisioning and patching Deployment Procedures. In particular, this appendix covers the following:

- [Troubleshooting Database Provisioning Issues](#)
- [Troubleshooting Linux Provisioning Issues](#)
- [Troubleshooting Patching Issues](#)
- [Troubleshooting Linux Patching Issues](#)
- [Troubleshooting Oracle Site Guard Issues](#)
- [Frequently Asked Questions on Linux Provisioning](#)
- [Refreshing Configurations](#)
- [Reviewing Log Files](#)

E.1 Troubleshooting Database Provisioning Issues

This section provides troubleshooting tips for common database provisioning issues.

E.1.1 Grid Infrastructure Root Script Failure

Issue

Grid Infrastructure root script fails.

Description

After Grid Infrastructure bits are laid down, the next essential step is Grid Infrastructure root script execution. This is the most process intensive phase of your deployment procedure. During this process, the GI stack configures itself and ensures all subsystems are alive and active. The root script may fail to run.

Solution

1. Visit each node that reported error and run the following command on n-1 nodes:

```
$GI_ORACLE_HOME/crs/install/rootcrs.pl -deconfig -force
```

2. If the root script did not run successfully on any of the nodes, pass the `-lastNode` switch on nth node (conditionally) to the final invocation as shown below.

```
$GI_ORACLE_HOME/crs/install/rootcrs.pl -deconfig -force -lastNode
```

Now, retry the failed step from the Procedure Activity page.

E.1.2 SUDO Error During Deployment Procedure Execution

Issue

A SUDO error occurs while performing a deployment.

Description

While performing a deployment, all `root`-related operations are performed over `sudo`. To improve security, production environments tend to fortify `sudo`. Therefore, you may encounter errors related to `sudo`.

Solution

Make the following changes in your sudoer's file:

1. Remove entry `Default requiretty`, if it exists in your sudoer's file.
2. If sudoers file contains entry `Default env_reset`, add the following entries after this parameter:

```
Defaults env_keep="JRE_HOME PERL5LIB EMDROOT"
```

E.1.3 Prerequisites Checks Failure

Issue

Prerequisites checks fail when submitting a deployment procedure

Cause

Perform a meticulous analysis of output from prerequisite checks. While most prerequisite failures are automatically fixed, it is likely that the deployment procedure failed due to auto-fix environment requirements. Some likely cases are:

- Group membership for users that are not local to the system. Since users are registered with a directory service, even root access does not enable the deployment procedure to alter their attributes.
- Zone separation in Solaris. If the execution zone of deployment procedure does not have privilege to modify system attributes, auto-fix operations of the deployment procedure will fail.

Solution

Ensure that the deployment procedure has appropriate privileges.

E.1.4 Oracle Automatic Storage Management (Oracle ASM) Disk Creation Failure

Issue

Oracle ASM disk creation fails

Cause

ASM disks tend to be used and purged over time. If an ASM instance is purged and physical ASM disks are left in their existing spurious state, they contain diskgroup information that can interfere with future ASM creation. This happens if the newly

created ASM uses the same diskgroup name as exists in the header of such a raw disk. If such a spurious disk exists in the disk discovery path of the newly created ASM it will get consumed and raise unexpected error.

Solution

Ensure that disk discovery path is as restrictive as possible. Also, ASM disks should be zeroed out as soon as ASM is being purged. Deployment procedures that support post 11.2 RDBMS have elaborate checks to detect the use case and warn the user beforehand.

E.1.5 Oracle ASM Disk Permissions Error

Issue

Encountered an Oracle ASM Disk permissions error

Description

Unlike NFS mounted storage wherein permissions set on any one node are visible throughout, ASM diskgroups require permissions to be set to each raw disk for all participating nodes.

Solution

For all participating nodes of the cluster, set 660 permissions to each raw disk being consumed.

E.1.6 Specifying a Custom Temporary Directory for Database Provisioning

To specify a temporary directory other than `/tmp` for placing binaries when provisioning databases, follow these steps:

1. Log in as a designer, and from the **Enterprise** menu, select **Provisioning and Patching**, then select **Database Provisioning**.
2. In the Database Procedures page, select the **Provision Oracle Database Deployment Procedure** and click **Create Like**.
3. In the Create Like Procedure page, in the General Information tab, provide a name for the deployment procedure.

In the Procedure Utilities Staging Path, specify the directory you want to use instead of `/tmp`, for example, `/u01/working`.

4. Click **Save**.

Use this deployment procedure for provisioning your Oracle databases.

E.1.7 Incident Creation When Deployment Procedure Fails

Issue

During deployment procedure execution, the steps to create database and Oracle ASM storage fails.

Solution

When a step in a deployment procedure executes successfully, it returns a positive exit code. If the step fails, and the exit code is not positive, it raises an incident which is stored in the OMS. All the associated log files and diagnosability information such as

memory usage, disk space, running process info and so on are packaged and stored. You can access the Incident Console and package this information as a Service Request and upload it to My Oracle Support. Click Help on the Incident Manager page for more information on creating a new Service Request.

E.1.8 Reading Remote Log Files

Explanation

In deployment procedure execution page, all remote log files relevant to the provisioning operation are displayed as hyperlinks in the job step. You can click on these hyperlinks and view the remote logs. The remote logs are stored in the OMS repository and can be accessed by My Oracle Support when troubleshooting.

E.1.9 Retrying Failed Jobs

Issue

Deployment procedure execution fails

Solution

If you deployment procedure execution has failed, check the job run details. You can retry a failed job execution or choose to ignore failed steps. For example, if your deployment procedure execution failed due to lack of disk space, you can delete files and retry the procedure execution. For certain issues which may not affect the overall deployment procedure execution, such as cluvy check failure, you may want to ignore the failed step and run the deployment procedure.

Retrying a job execution creates a new job execution with the status **Running**. The status of the original execution is unchanged.

To ignore a failed step and retry the procedure, follow these steps:

1. In the Procedure Activity page, click on the relevant procedure.
2. In the Job Status page, click on the status of the failed step.
3. In the Step Status page, click **Ignore**. In the Confirmation page, click **Yes**.
4. Click **Retry**. The failed step will be retried.

E.2 Troubleshooting Patching Issues

This section provides troubleshooting tips for common patching issues.

- [Oracle Software Library Configuration Issues](#)
- [My Oracle Support Connectivity Issues](#)
- [Host and Oracle Home Credential Issues](#)
- [Collection Issues](#)
- [Patch Recommendation Issues](#)
- [Patch Plan Issues](#)
- [Patch Plan Analysis Issues](#)
- [User Account and Role Issues](#)

E.2.1 Oracle Software Library Configuration Issues

This section describes the following patching issues:

- [Error Occurs While Staging a File](#)
- [Error Occurs While Uploading a Patch Set](#)

E.2.1.1 Error Occurs While Staging a File

Issue

While analyzing the patch plan, the patch plan fails with an unexpected error, although the credentials are correct and although you have write permission on the EM stage location.

For example, the following error is seen on job output page:

```
"Unexpected error occurred while checking the Normal Oracle Home Credentials"
```

Cause

You might have set up the Software Library using the OMS Agent file system, and you might not have access to the named credentials that were used for setting up the Software Library.

Solution

To resolve this issue, explicitly grant yourself access to the named credentials that were used to set up the Software Library.

E.2.1.2 Error Occurs While Uploading a Patch Set

Issue

When you upload a patch set using the Upload Patches to Software Library page, you might see an error stating that the operation failed to read the patch attributes.

For example,

```
ERROR:Failed to read patch attributes from the uploaded patch file <filename>.zip
```

Cause

Although you upload a metadata file along with a patch set ZIP file, sometimes the patch attributes are not read from the metadata file. As a result, the operation fails stating that it could not read the attributes.

Solution

To resolve this issue, manually enter all the patch attributes in the Patch Information section of the Upload Patches to Software Library page. For example, patch number, created on, description, platform, and language.

E.2.1.3 OPatch Update Job Fails When Duplicate Directories Are Found in the Software Library

Issue

When you run an OPatch Update job, sometimes it might fail with the following error:

```
2011-11-28 10:31:19,127 RemoteJobWorker 20236 ERROR em.jobs startDownload.772-  
OpatchUpdateLatest: java.lang.NullPointerException: Category, 'Oracle Software
```

```
Updates', has no child named, 'OPatch' at  
oracle.sysman.emInternalSDK.core.patch.util. ComponentUtil.getComponentCategory  
(ComponentUtil.java:854)
```

Even after applying the Cloud Control patch released in January 2012, you might see the following error:

```
Category, 'Oracle Software Updates' already exists.
```

Cause

The error occurs when two *Patch Components* directories are found in the Software Library. Particularly when you run two patch upload or download jobs, for example, an OPatch patch download job and a regular patch download job, a race condition is created, which in turn creates two directories with the name *Patch Components*. The Software Library does not display any error while creating these duplicate directories, but when you run the OPatch Update job, the job fails with a `NullPointerException`.

Solution

To resolve this issue, do one of the following:

If you see two *Patch Components* directories in the Software Library, then delete the one that has fewer entries, and retry the failed patch upload or download job. To access the Software Library, from the **Enterprise** menu, select **Provisioning and Patching**, and click **Software Library**.

If you see only one *Patch Components* directory, but yet see the error that states that the Oracle Software Updates already exists, then retry the failed patch upload or download.

E.2.2 My Oracle Support Connectivity Issues

This section describes the following issues:

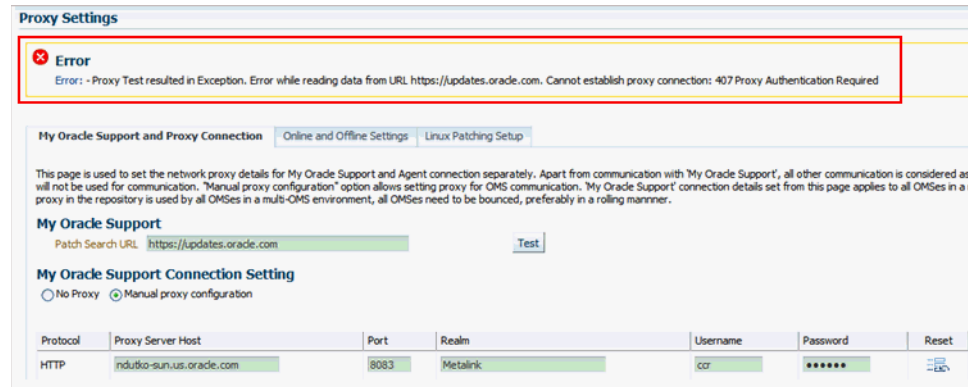
- [Error Occurs While Testing the Proxy Server That Supports Only Digest Authentication](#)

E.2.2.1 Error Occurs While Testing the Proxy Server That Supports Only Digest Authentication

Issue

On the Proxy Settings page, in the My Oracle Support and Proxy Connection tab, when you provide the manual proxy configuration details, you might see an exception error as shown in [Figure E-1](#).

Figure E-1 Proxy Settings Error



Cause

You might have provided the configuration details of a proxy server that supports only the *Digest* authentication schema. By default, the proxy server is mapped only to the *Basic* authentication schema, and currently there is no support for *Digest* authentication schema.

Solution

To resolve this issue, reconfigure your proxy server to make it to use the *Basic* authentication schema.

Tip: For better understanding of connectivity issues related to HTTP Client Logging, you can perform the following steps:

1. Locate the `startup.properties` file under the GC instance directory:
`user_projects/domains/EMGC_DOMAIN/servers/EMGC_OMS1/data/nodemanager/startup.properties`
2. Append the following string to the value of the property **Arguments**:
`-DHTTPClient.log.level\=ALL`
`-DHTTPClient.log.verbose\=true`
3. Restart the OMS, and the WebLogic Server Administration Manager by running the following commands:
`emctl stop oms -all`
`emctl start oms`
4. Navigate to the following location to check the log file:
`user_projects/domains/EMGC_DOMAIN/servers/EMGC_OMS1/logs/EMGC_OMS1-diagnostic.log`

Alternately, you can also use the **grep** command to find all the HTTP connection logs as follows:

```
grep HTTPClient EMGC_OMS1-diagnostic*.log
```

E.2.3 Host and Oracle Home Credential Issues

This section describes the following security issues:

- [Cannot Create Log Files When You Set Privileged Credentials as Normal Oracle Home Credentials](#)

E.2.3.1 Cannot Create Log Files When You Set Privileged Credentials as Normal Oracle Home Credentials

Issue

While creating a patch plan, if you choose to override the Oracle home preferred credentials, and set privileged credentials as normal Oracle home credentials inadvertently as shown in [Figure E-2](#), then you will see an error stating that log files cannot be created in the EMStagedPatches directory.

For example,

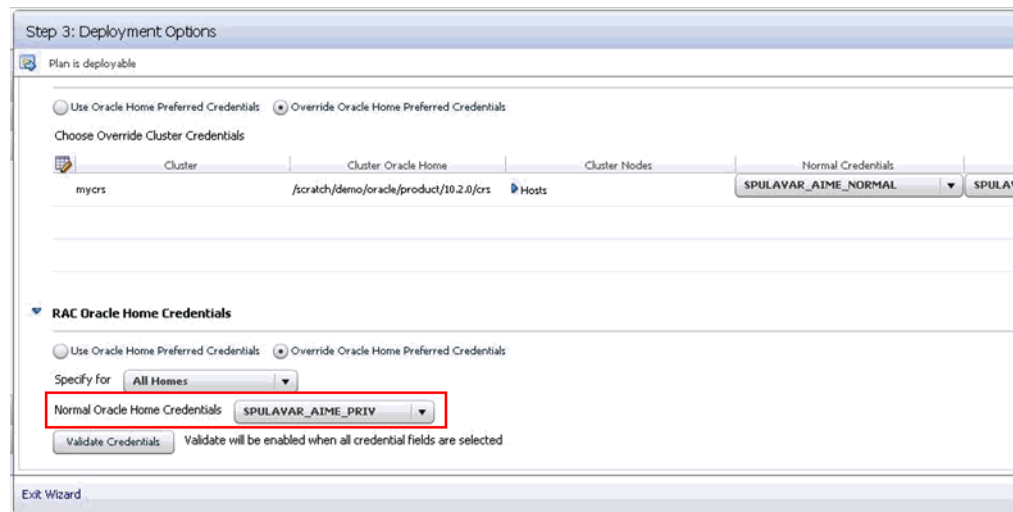
```
"Unable to create the file <RAC_HOME>/EMStagedPatches/PA_APPLY_PATCH_09_02_2011_14_27_13.log"
```

You might also see the following error:

```
ERROR: SharedDeviceException.
```

```
ACTION: Please check whether the configuration is supported or not.
```

Figure E-2 Inadvertently Selecting Privileged Credentials as Normal Credentials



Cause

When a patch plan is deployed, the patch plan internally uses a deployment procedure to orchestrate the deployment of the patches. While some of the steps in the deployment procedure are run with normal Oracle home credentials, some of the steps are run with privileged Oracle home credentials. However, when you set normal Oracle home credentials as privileged Oracle home credentials, then the deployment procedure runs those steps as a root user instead of the Oracle home owner, and as a result, it encounters an error.

Solution

To resolve this issue, return to the Create Plan Wizard, in the Deployment Options page, in the Credentials tab, set normal credentials as normal Oracle home credentials.

E.2.4 Collection Issues

This section describes the following issues:

- [Missing Details in Plan Wizard](#)
- [Cannot Add Targets to a Patch Plan](#)

E.2.4.1 Missing Details in Plan Wizard

Issue

When you view a patch plan, sometimes the Create Plan Wizard does not display the expected information. Some pages or sections in the wizard might be blank.

Cause

The issue might be with the details in the Management Repository or with the Create Plan Wizard.

Solution

Identify whether the issue is with the Management Repository or with the Create Plan Wizard. To do so, try retrieving some details from the Management Repository using the commands and URLs mentioned in this section.

- If the URLs return the correct information but the console does not display it, then there might be some technical issue with the Create Plan Wizard. To resolve this issue, contact Oracle Support.
- If the URLs return incorrect information, then there might be some issue with the Management Repository. To resolve this issue, re-create the patch plan.

To retrieve some details from the Management Repository, do the following:

- Retrieve the GUID of the patch plan. To do so, run the following command:

```
select plan_guid from em_pc_plans where name='<name of the
plan>';
```

For example,

```
select plan_guid from em_pc_plans where name='t8';
```

The result of the command looks like the following. Note down the GUID of the plan.

```
PLAN_GUID
-----
96901DF943F9E3A4FF60B75FB0FAD62A
```

- Retrieve general information about a patch plan such as its name, type, status, and plan privileges. To do so, use the following URL. This type of information is useful for debugging the *Plan Information* step and the *Review and Deploy* step.

```
https://<hostname>:<port>/em/console/CSP/main/patch/plan?plan
Id=<plan_guid>&client=emmos&cmd=get&subset=planInfo
```

Note: Before retrieving any information about a patch plan using the preceding URL, log in to the Cloud Control console, and from the **Enterprise** menu, select **Provisioning and Patching**, and then click **Patches & Updates**.

- Retrieve information about the patches and the associated targets that are part of the patch plan. To do so, use the following URL. This type of information is useful for debugging the *Patches* step and the *Review* step.

`https://<hostname>:<port>/em/console/CSP/main/patch/plan?planId=<plan_guid>&client=emmos&cmd=get&subset=patches`

- Retrieve information about the deployment options selected in the patch plan. To do so, use the following URL. This type of information is useful for debugging the *Deployment Options* step and the *Credentials* step.

`https://<hostname>:<port>/em/console/CSP/main/patch/plan?planId=<plan_guid>&client=emmos&cmd=get&subset=deploymentOptions`

- Retrieve information about the preferred credentials set in the patch plan. To do so, use the following URL. This type of information is useful for debugging the *Credentials* step.

`https://<hostname>:<port>/em/console/CSP/main/patch/plan?planId=<plan_guid>&client=emmos&cmd=get&subset=preferredCredentials`

- Retrieve information about the target credentials set in the patch plan. To do so, use the following URL. This type of information is useful for debugging the *Credentials* step.

`https://<hostname>:<port>/em/console/CSP/main/patch/plan?planId=<plan_guid>&client=emmos&cmd=get&subset=targetCredentials`

- Retrieve information about the conflict-free patches in the patch plan. To do so, use the following URL. This type of information is useful for debugging the *Validation* step and the *Review & Deploy* step.

`https://<hostname>:<port>/em/console/CSP/main/patch/plan?planId=<plan_guid>&client=emmos&cmd=get&subset=conflictFree`

- Retrieve information about the suppressed patches in the patch plan. To do so, use the following URL. This type of information is useful for debugging the *Patches* step.

`https://<hostname>:<port>/em/console/CSP/main/patch/plan?planId=<plan_guid>&client=emmos&cmd=get&subset=removedPatchList`

E.2.4.2 Cannot Add Targets to a Patch Plan

Issue

While creating a new patch plan or editing an existing patch plan, when you add a new target, you might see the following error:

```
Wrong Platform. Expected: Oracle Solaris on SPARC (64-bit), found: null
```

Cause

The Management Repository might not have the platform information for that target. By default, for every target, the inventory details are regularly collected from the `oraclehomeproperties.xml` file that resides in the Oracle home of the target.

Sometimes, the inventory collection might not have completed or might have failed, resulting in missing data in the Management Repository. Due to these reasons, you might not be able to add those targets.

Solution

To resolve this issue, forcefully recollect the inventory details from the Oracle home of the target.

To retrieve the Oracle home details, follow these steps:

1. From the **Targets** menu, select **All Targets**.
2. On the All Targets page, from the left hand **Refine Search** pane, click **Target Type** menu to expand it.
3. From the Target Type, click **Others**, select **Oracle Home**.
4. All the targets of type Oracle Home are listed. You may search for the host name to drill down to the Oracle home details you are looking for.

To retrieve the inventory details from the Oracle Home on the target host, run the following command from the \$EMDR00T/bin directory:

```
$ emctl control agent runCollection <Oracle_Home_Target>:oracle_home oracle_home_config
```

Here, <Oracle_Home_Target> refers to the name of the Oracle home of the target whose platform information is missing.

For example,

```
$ emctl control agent runCollection db2_2_adc2170603:oracle_home oracle_home_config
```

E.2.5 Patch Recommendation Issues

This section describes the following issues:

- [Patch Recommendations Do Not Appear After Installing Oracle Management Agent on Oracle Exadata Targets](#)

E.2.5.1 Patch Recommendations Do Not Appear After Installing Oracle Management Agent on Oracle Exadata Targets

Issue

After installing the Management Agent on Oracle Exadata targets, the patch recommendations do not appear.

Cause

The patch recommendations do not appear because the Exadata plug-ins are not deployed.

Solution

To resolve this issue, explicitly deploy the Exadata plug-ins on Exadata targets. To do so, follow these steps:

1. From the **Enterprise** menu, select **Extensibility**, then select **Plug-ins**.

2. On the Plug-ins page, in the table, select the Oracle Exadata plug-in version you want to deploy.
3. Click **Deploy On** and select **Management Agent**.
4. In the Deploy Plug-in on Management Agent dialog, in the Selected Management Agent section, click **Add** and select one or more Management Agents where you want to deploy the plug-in, and click **Continue**. Then click **Next**, then **Deploy**.

E.2.6 Patch Plan Issues

This section describes the following issues:

- [Patch Plan Becomes Nondeployable and Fails](#)
- [Instances Not to Be Migrated Are Also Shown as Impacted Targets for Migration](#)
- [Cluster ASM and Its Instances Do Not Appear as Impacted Targets While Patching a Clusterware Target](#)
- [Recovering from a Partially Prepared Plan](#)
- [Error #1009 Appears in the Create Plan Wizard While Creating or Editing a Patch Plan](#)
- [Analysis Succeeds But the Deploy Button is Disabled](#)
- [Patch Plan Fails When Patch Plan Name Exceeds 64 Bytes](#)
- [Out-of-Place Patching Fails for 11.2.0.3 Exadata Clusterware](#)

E.2.6.1 Patch Plan Becomes Nondeployable and Fails

Issue

The patch plan fails stating it is a nondeployable plan.

Cause

You can add a patch to a target in a patch plan only if the patch has the same release and platform as the target to which it is being added. You will receive a warning if the product for the patch being added is different from the product associated with the target to which the patch is being added. The warning does not prevent you from adding the patch to the patch plan, though. However, when you try to deploy, the plan might fail.

Solution

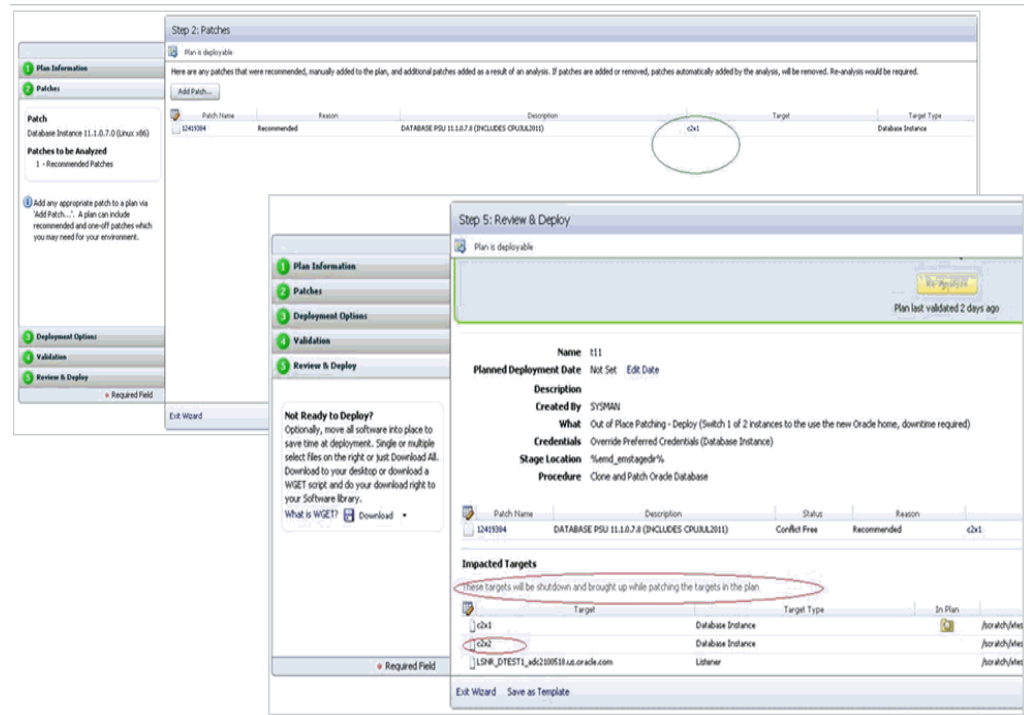
To make a nondeployable patch plan deployable, divide the patch plan into smaller deployable plans that contain only homogenous patches and targets.

E.2.6.2 Instances Not to Be Migrated Are Also Shown as Impacted Targets for Migration

Issue

When you deploy a patch plan in out-of-place patching mode, sometimes even the instances that are not selected for migration are identified as impacted targets as shown in [Figure E-3](#).

Figure E-3 Instances Not to Be Migrated Are Shown as Impacted Targets



Cause

By default, the patch plan calculates the impacted targets based on only one mode, which in-place patching mode. Therefore, although you have selected out-of-patching mode, the patch plan ignores it and considers only the in-place patching mode as the option selected, and displays all the targets as impacted targets for migration.

Solution

To resolve this issue, ignore the targets you have not selected for migration. They will not be shut down or migration in any case.

E.2.6.3 Cluster ASM and Its Instances Do Not Appear as Impacted Targets While Patching a Clusterware Target

Issue

While creating a patch plan for patching a clusterware target, on the Deployment Options page, the What to Patch section does not display the cluster ASM and its instances as affected targets. They do not appear in the Impacted Targets section, either. And after deploying the patch plan in out-of-place mode, the cluster ASM and its instances show metric collection error.

Cause

This issue might occur if the clusterware target name in Cloud Control and the clustername target name in the mgmt\$target_properties table are not matching.

Solution

To resolve this issue, run the following query to verify the target property ClusterName of the clusterware target:

```
select property_value from mgmt$target_properties where target_
name=<CRS Target Name> and property_name="ClusterName"
```

If the returned value is different from the clusterware target name in Cloud Control, then delete the clusterware target and other associated targets, and rediscover them. This time while rediscovering them, ensure that the clusterware target name matches with the name returned by the preceding query.

E.2.6.4 Recovering from a Partially Prepared Plan

Issue

When you create a patch plan to patch multiple Oracle homes in out-of-place patching mode, and when you click **Prepare** in the Create Plan Wizard to prepare the patch plan before actually deploying it, sometimes the preparation operation fails with the message *Preparation Failed*.

Cause

The patch plan might have successfully cloned and patched some of the selected Oracle homes, but might have failed on a few Oracle homes. The overall status of the patch plan is based on the patching operation being successful on all the Oracle homes. Even if the patching operation succeeds on most of the Oracle homes and fails only on a few Oracle homes, the overall status is shown as if the patch plan has failed in one of the steps.

Solution

To resolve this issue, fix the errors on failed Oracle homes. Then, go to the procedure instance page and retry the failed steps.

E.2.6.5 Error #1009 Appears in the Create Plan Wizard While Creating or Editing a Patch Plan

Issue

While creating new patch plan or editing an existing patch plan, you might see the following error in the Create Plan Wizard:

```
Error #1009
```

Cause

This error occurs while accessing the Management Repository to extract any details about the patch plan, the targets, or the operation being committed. Usually, `SQLException`, `NullPointerException`, or `Unhandled exceptions` cause these errors.

Solution

To resolve this issue, review the following file, make a note of the exact error or exception logged, and communicate it to Oracle Support.

```
$MIDDLEWARE_HOME/gc_inst/em/EMGC_OMS1/sysman/log/emoms.log
```

E.2.6.6 Analysis Succeeds But the Deploy Button is Disabled

Issue

After you successfully analyze the patch plan, when you navigate to the Review of the Create Plan Wizard, you might see the **Deploy** button disabled. Also, the table on the

Review page appears empty (does not list any patches.) As a result, you might not be able to deploy the patch plan.

Cause

This error occurs if the patches in the patch plan have already been applied on the target Oracle home. In such a case, the Validation page confirms that the patches have already been applied and therefore they have been skipped, and on the Review page, Deploy button is disabled.

Solution

The patches have already been applied, so you do not have to apply them again. If required, you can manually roll back the patch from the target Oracle home and try applying the patch again.

E.2.6.7 Patch Plan Fails When Patch Plan Name Exceeds 64 Bytes

Issue

On non-English locales, patch plans with long plan names fail while analyzing, preparing, or deploying, or while switching back. No error is displayed; instead the patch plan immediately reflects the *Failed* state, and logs an exception in the `<INSTANCE_HOME>/sysman/log/emoms.log` file.

Cause

The error occurs if the patch plan name is too long, that is, if it exceeds 64 bytes. The provisioning archive framework has a limit of 64 bytes for instance names, and therefore, it can accept only plan names that are lesser than 64 bytes. Typically, the instance name is formed using the patch plan name, the plan operation, and the time stamp (PlanName_PlanOperation_TimeStamp). If the entire instance name exceeds 64 bytes, then you are likely see this error.

Solution

To resolve this issue, do one of the following:

If the patch plan failed to analyze, prepare, or deploy, then edit the plan name and reduce its length, and retry the patching operation.

If the patch plan was deployed successfully, then the patch plan gets locked, and if switchback fails with this error, then you cannot edit the plan name in the wizard. Instead, run the following SQL update command to update the plan name in the Management Repository directly:

```
update em_pc_plans set name = 'New shorter name' where name =
'Older longer name';
commit;
```

E.2.6.8 Out-of-Place Patching Fails for 11.2.0.3 Exadata Clusterware

Issue

The out-of-place patching fails to unlock the cloned Oracle home in the *Prepare* phase of the patch plan, thus causing the patch plan to fail on the cloned Oracle home. The step *Run clone.pl on Clone Oracle Home* fails.

Cause

This issue occurs if the new Oracle home is different from the Oracle home mentioned in the files `<gi_home>/crs/utl/crsconfig_dirs` and `crsconfig_fileperms` that are present in the Grid Infrastructure home. For 11.2.0.3 Exadata Clusterware, the unlock framework works by operating on these files.

Solution

To resolve this issue, you can do one of the following:

- Create a new patch plan for the Exadata Cluster, select the required patch, select **In-Place** in the How to Patch section, and deploy the patch plan.
- Manually apply the patch on the Clusterware Oracle homes of all the nodes of the cluster. Then, clean up the partially cloned Oracle homes on all the nodes, and retry the *Prepare* operation from the patch plan.

E.2.7 Patch Plan Analysis Issues

This section covers the following issues:

- [Patch Plan Remains in Analysis State Even After the Deployment Procedure Ends](#)
- [Patch Plan Analysis Fails When the Host's Node Name Property Is Missing](#)
- [Link to Show Detailed Progress on the Analysis Is Not Actionable](#)
- [Raising Service Requests When You Are Unable to Resolve Analysis Failure Issues](#)

E.2.7.1 Patch Plan Remains in Analysis State Even After the Deployment Procedure Ends

Issue

When you analyze a patch plan, sometimes the patch plan shows that analysis is in progress even after the underlying deployment procedure or the job ended successfully.

Cause

This issue can be caused due to one of the following reasons:

- Delayed or no notification from the job system about the completion of the deployment procedure. Typically, after the deployment procedure ends, the job system notifies the deployment procedure. Sometimes, there might be a delay in such notification or there might be no notification at all from the job system, and that can cause the status of the patch plan to show that is always in the analysis state.
- Delay in changing the status of the patch plan. Typically, after the job system notifies the deployment procedure about its completion, the job system submits a new job to change the status of the patch plan. Sometimes, depending on the load, the new job might remain the execution queue for a long time, and that can cause the status of the patch plan to show that is always in the analysis state.
- Failure of the job that changes the status of the patch plan. Sometimes, after the new job is submitted for changing the status of the patch plan, the new job might fail if there are any Management Repository update issues or system-related issues.
- Time zone issues with the Management Repository. If the Management Repository is configured on an Oracle RAC database, and if each instance of the Oracle RAC

is running on a different time zone, then when a query is run to know the current system time, it can return incorrect time details depending on which instance serviced the request. Due to incorrect time details, the job that changes the status of the patch plan might not run at all. This can cause the status of the patch plan to show that is always in the analysis state.

Solution

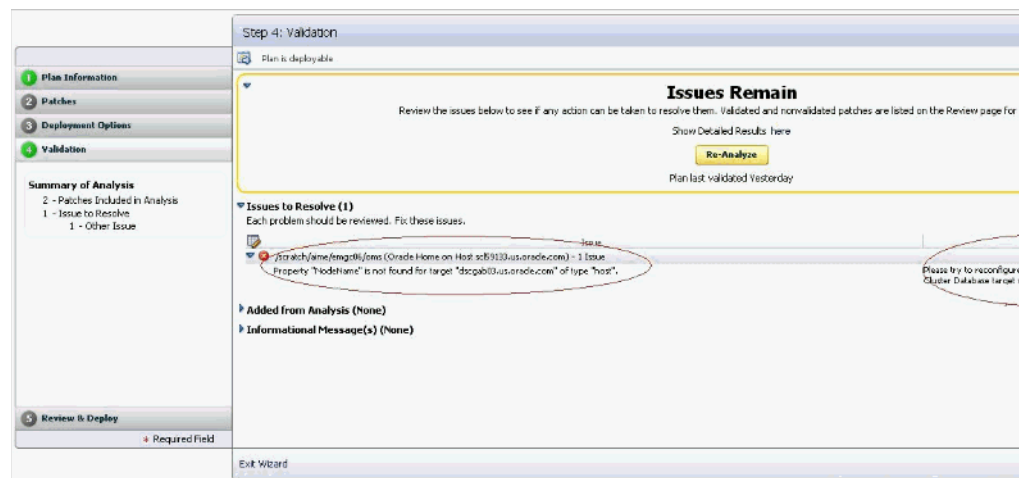
For time zone-related issue, then first correct the time zone settings on the Oracle RAC nodes, and then restart them. For all other issues, collect the logs and contact Oracle Support.

E.2.7.2 Patch Plan Analysis Fails When the Host's Node Name Property Is Missing

Issue

When you validate a patch plan created for patching Oracle Clusterware, the validation fails as shown in [Figure E-4](#), stating that the node name is missing for the target `<target_name>` of the type `host`. Also, the solution mentioned on the Validation page is incorrect.

Figure E-4 Analysis Fails Stating Node Name Property Is Missing for a Target



Cause

The error occurs because the Create Plan Wizard does not sync up with the actual query or the job you are running. Also, the property `nodeName` is a dynamic property for `HAS` target, which is not marked as a critical property, and therefore, this property could be missing from the Management Repository sometimes. Ideally, it should state that the node name property is missing for the `HAS` target.

Solution

To resolve this issue, run the following command to reload the dynamic properties for the `HAS` target from each node of the Oracle Clusterware.

```
emctl reload dynamicproperties -upload_timeout 600 <target_name>:has
```

For example,

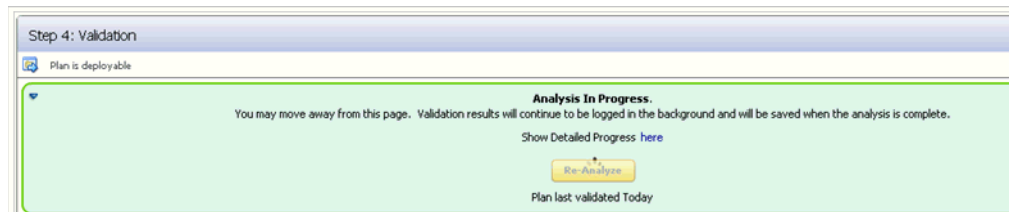
```
emctl reload dynamicproperties -upload_timeout 600 <myhastarget1>:has
```

E.2.7.3 Link to Show Detailed Progress on the Analysis Is Not Actionable

Issue

After you analyze a patch plan, the text *Analysis In Progress* on the Validation page appears smaller than normal, and the *here* link for progress details does not work as shown in [Figure E-5](#).

Figure E-5 Link to Show Detailed Progress Appears Broken



Cause

You see this error because of a technical issue in rendering this link.

Solution

To resolve this issue, exit the Create Plan Wizard. On the Patches & Updates page, in the **Plans** region, click on the status **Analysis in Progress** against the patch plan where you faced this issue.

E.2.7.4 Raising Service Requests When You Are Unable to Resolve Analysis Failure Issues

As described in the preceding subsections, there can be several causes for analysis failures, including My Oracle Support connectivity issues, ARU issues, or issues while accessing the Management Repository to extract any details related to the patch plan or targets or the operation being committed. If you encounter any of these issues, follow the solution proposed in the preceding sections, and if you are still unable to resolve the issue, follow these steps, and raise a service request or a bug with the information you collect from the steps.

- *(Online Mode Only)* Verify if the My Oracle Support Web site being used is currently available.
- *(Online Mode Only)* If the plan analysis is failing prior to target analysis being submitted, then verify if the patch analysis is working as expected by running the following URL Replace `<em_url>` with the correct EM URL, and `<plan_name>` with the actual patch plan name.

`<em_url>/em/console/CSP/main/patch/plan?cmd=getAnalysisXML&type=att&planName=<plan_name>`

 Verify if the returned XML includes conflict check request and response XMLs for each Oracle home included in the patch plan.
- Open the following file and check the exact error or exception being logged and communicate it to Oracle Support.

`$(MIDDLEWARE_HOME)/gc_inst/em/EMGC_OMS1/sysman/log/emoms.log`

E.2.8 User Account and Role Issues

This section describes the following:

- [Out-of-Place Patching Errors Out If Patch Designers and Patch Operators Do Not Have the Required Privileges](#)

E.2.8.1 Out-of-Place Patching Errors Out If Patch Designers and Patch Operators Do Not Have the Required Privileges

Issue

When you try out-of-place patching, the patch plan fails with the following error while refreshing the Oracle home configuration:

```
12:58:38 [ERROR] Command failed with error: Can't deploy oracle.sysman.oh on
https://<hostname>:<port>/emd/main/
```

Cause

The error occurs because you might not have the following roles as a *Patch Designer* or a *Patch Operator*:

- **ORACLE_PLUGIN_USER**, to view the plug-in user interface
- **ORACLE_PLUGIN_OMS_ADMIN**, to deploy a plug-in on the OMS
- **ORACLE_PLUGIN_AGENT_ADMIN**, to deploy a plug-in on the Management Agent

These roles are required to submit the *Discover Promote Oracle Home Targets* job. The job deploys the Oracle home plug-in on the Management Agent if it is not already deployed.

Solution

Grant these roles explicitly while creating the user accounts. Alternatively, grant the provisioning roles because **EM_PROVISIONING_OPERATOR** and **EM_PROVISIONING_DESIGNER** already include these roles. After granting the privileges, retry the failed deployment procedure step to complete the out-of-patching preparation.

E.3 Troubleshooting Linux Patching Issues

My Staging Server Setup DP fails at "Channels Information Collection" step with the error message "Could not fetch the subscribed channels properly". How do I fix this?

This error is seen if there is any network communication error between up2date and ULN. Check if up2date is configured with correct proxy setting by following https://linux.oracle.com/uln_faq.html - 9. You can verify if the issue is resolved or not by using the command, `up2date -nox -show-channels`. If the command lists all the subscribed channels, the issue is resolved.

My "up2date -nox -show-channels" command does not list the subscribed channels properly. How do I fix this?

Go to `/etc/sysconfig/rhn/sources` files, uncomment `up2date default` and comment out all the local RPM Repositories configured.

How can I register to channels of other architectures and releases?

Refer to https://linux.oracle.com/uln_faq.html for this and more such related FAQs.

After visiting some other page, I come back to "Setup Groups" page; I do not see the links to the jobs submitted. How can I get it back?

Click Show in the details column.

Package Information Job fails with "ERROR: No Package repository was found" or "Unknown Host" error. How do I fix it?

Package Repository you have selected is not good. Check if metadata files are created by running `yum-arch` and `createrepo` commands. The connectivity of the RPM Repository from OMS might be a cause as well.

Even after the deployment procedure finished its execution successfully, the Compliance report still shows my Group as non-compliant, why?

Compliance Collection is a job that runs once in every 24 hour. You should wait for the next cycle of the job for the Compliance report to update itself. Alternately, you can go to the **Jobs** tab and edit the job to change its schedule.

Package Information Job fails with "ERROR: No Package repository was found" or "Unknown Host" error. How do I fix it?

The package repository you have selected is not good. Check if the metadata files are created by running `yum-arch` and `createrepo` commands. The connectivity of the RPM Repository from OMS might be a cause as well.

I see a UI error message saying "Package list is too long". How do I fix it?

Deselect some of the selected packages. The UI error message tells you from which package to unselect.

E.4 Troubleshooting Linux Provisioning Issues

I cannot see my stage, boot server in the UI to configure them with the provisioning application?

Either Management Agents have not been installed on the Stage or Boot Server machine, or it is not uploading data to the OMS. Refer to the *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide* for troubleshooting information and known issues.

Bare metal machine is not coming up since it cannot locate the Boot file.

Verify the dhcp settings (`/etc/dhcpd.conf`) and tftp settings for the target machine. Check whether the services (dhcpd, xinted, portmap) are running. Make the necessary setting changes if required or start the required services if they are down.

Even though the environment is correctly setup, bare metal box is not getting booted over network

OR

DHCP server does not get a DHCPDISCOVER message for the MAC address of the bare metal machine.

Edit the DHCP configuration to include the IP address of the subnet where the bare metal machine is being booted up.

Agent Installation fails after operating system has been provisioned on the bare metal box?

OR

No host name is assigned to the bare metal box after provisioning the operating system?

This might happen if the `get-lease-hostnames` entry in the `dhcpd.conf` file is set to `true`. Edit the `dhcpd.conf` file to set `get-lease-hostnames` entry to `false`.

Also, ensure that length of the host name is compatible with length of the operating system host name.

Bare metal machine hangs after initial boot up (tftp error/kernel error).

This may happen if the tftp service is not running. Enable the tftp service. Go to the `/etc/xinetd.d/tftp` file and change the `disable` flag to `no` (`disable=no`). Also verify the dhcp settings.

Kernel panic occurs when the Bare Metal machine boots up.

Verify the dhcp settings and tftp settings for the target machine and make the necessary changes as required. In a rare case, the `initrd` and `vmlinuz` copied may be corrupted. Copying them from RPM repository again would fix the problem.

Bare metal machine hangs after loading the initial kernel image.

This may happen if the network is half duplex. Half duplex network is not directly supported but following step will fix the problem:

- Modify `ethtool -s eth0 duplex half` to `ethtool -s eth0 duplex full` in the kickstart file.

Bare metal machine cannot locate the kickstart file (Redhat screen appears for manually entering the values such as 'language', 'keyboard' etc).

This happens if `STAGE_TOP_LEVEL_DIRECTORY` is not mountable or not accessible. Make sure the stage top level is network accessible to the target machine. Though very rare but this might also happen because of any problem in resolving the stage server hostname. Enter the IP address of the stage or the NAS server instead of hostname on which they are located, and try the provisioning operation again.

Bare metal machine does not go ahead with the silent installation (Redhat screen appears for manually entering the network details).

Verify that DNS is configured for the stage server host name, and that DHCP is configured to deliver correct DNS information to the target machine. If the problem persists, specify the IP address of the stage or NAS server instead of hostname, and try the provisioning operation again.

After provisioning, the machine is not registered in Enterprise Manager.

This happens if Enterprise Manager Agent is not placed in the `STAGE_TOP_LEVEL_DIRECTORY` before provisioning operation. Place the Enterprise Manager agent in this directory, and try the operation again. It might also happen if the OMS registration

password provided for securing the agents is incorrect. Go to the agent oracle home on the target machine, and run the `emctl secure agent` command supplying the correct OMS registration password.

Check the time zone of the OMS and the provisioned operating system. Modify the time zone of the provisioned operating system to match with the OMS time zone.

With 64-bit OS provisioning, agent is not installed.

During OS provisioning, specify the full path of the agent RPM in the Advanced Operating System Properties page.

Provisioning operations cannot be initiated since either one or all of Stage Server, Boot Server, and RPM Repository have not been configured in the Infrastructure page.

Set up at least one stage server, boot server, and RPM repository to proceed with Linux Provisioning.

Submitting the deployment operations throws an error: "An unexpected error has occurred. Please check the log files for details." Logs have the corresponding message: "ComponentType with internal name BMPTType not found"

Set up Software Library from the Software Library console.

The deployment procedure fails with directory permission error.

This error occurs because of insufficient user privileges on the stage server machine. `STAGE_TOP_LEVEL_DIRECTORY` should have write permission for the stage server user. In case of NAS, the NAS directory should be mounted on the staging server. If the error appears while writing to the boot directory, then the boot server user must have the write permission.

Bare metal box fails to boot with "reverse name lookup failed" error.

Verify that the DNS has the entry for the IP address and the host name.

Fetching properties from reference machine throws the error: " Credentials specified does not have root access"

Verify if the credentials specified for the reference machine has `sudo` access.

Following Package/Package Group are not available in the RPM Repository. Either update the Package List or select the correct RPM Repository in the Deployment page.

Verify that the RPM packages mentioned in the error message are present in the repository, and that they are spelled correctly. If not, either copy the packages to the repository or do not install them.

E.5 Troubleshooting Oracle Site Guard Issues

This section describes common situations that you might encounter when deploying and managing Oracle Site Guard in disaster recovery topologies. It also explains the steps for addressing them.

E.5.1 Operation Plan Failure

This section provides tips for troubleshooting issues for operation plan failure.

Issue

Targets like Oracle Database or Oracle Fusion Middleware farm, which are part of the system, might not be discovered in the operation plan workflow.

Description and Solution

This problem may occur if you have added targets to the system after creating the operation plan. Oracle Site Guard only includes those targets that are part of the system during the creation of the operation plan. If you have added new targets, re-create the operation plan.

Issue

The Oracle WebLogic Server managed-server target, which is part of the Oracle WebLogic Server domain, is not updated or identified by Oracle Site Guard when creating the operation plan workflow.

Description and Solution

Ensure that the managed servers are running, before performing an automatic discovery in Enterprise Manager Cloud Control.

Issue

When an operation step (for example, database switchover or failover, custom scripts, and so on) hangs, manual intervention is needed.

Description and Solution

Suspend the operation from the Enterprise Manager Cloud Control console. Do not stop the operation.

After completing the manual procedures, resume the operation to complete the Oracle Site Guard operation. Do not re-submit the operation.

If Oracle Site Guard determines that the components are already in the desired state, it performs a 'no operation' for all the start or stop or database switchover operations. This appropriately ends the process, and updates the sites with the required roles. If an operation step fails, and if manual intervention is needed to resolve the issue, you can either retry the failed step or confirm the manual step, and proceed with the execution of the operation.

Note: Restart or resume the operation after every manual intervention. Ensure that you complete the operations that you have started.

Issue

OPMN Managed System Components which are part of the system might not be discovered in the operation plan workflow.

Description and Solution

Oracle Site Guard discovers only those OPMN managed system components represented in Enterprise Manager Cloud Control. For example, OPMN Managed System Components like Oracle HTTP Server and Oracle Web cache, are represented in Enterprise Manager Cloud Control. These components are discovered as part of the Oracle Fusion Middleware farm.

Issue

Oracle RAC Database, which is part of the system, may not be discovered in the operation plan workflow.

Description and Solution

Oracle RAC Databases are grouped and represented under RAC Database target in the Enterprise Manager Cloud Control. When RAC database instances are discovered, the RAC database target is created, and all the database instances in the RAC deployment are grouped under the RAC database target. This issue may occur if individual RAC instance targets are added to the system, instead of the RAC database target. Oracle Site Guard cannot identify individual RAC instances.

Issue

Site Guard operation step fails with the error `stageOmsFileEntry (Error)`, while using credentials with `sudo` privileges. You might encounter this issue during the precheck operation as well.

Description and Solution

When the credentials used by Site Guard are configured to use `sudo` privileges to run as `root`, the `sudo` privilege must be configured as PDP (Privilege Delegation Provider) on all the agents running on the respective hosts of the target.

PDP can be configured from Enterprise Manager Cloud Control console. To configure PDP, go to **Setup -> Security -> Privilege Delegation** in the Enterprise Manager Cloud Control console.

E.5.2 Switchover or Failover Operations Failure

This section provides tips for troubleshooting for issues that you may encounter during switchover or failover operations.

Issue

The Administration Server might not start after performing switchover or failover operation. The output log file of the Administration Server reports an error, such as the following:

```
<Jan 19, 2012 3:43:05 AM PST> <Warning> <EmbeddedLDAP> <BEA-171520> <Could not
obtain an exclusive lock for directory: ORACLE_
BASE/admin/soadomain/aserver/soadomain/servers/AdminServer/data/ldap/ldapfiles.
Waiting for 10 seconds and then retrying in case existing WebLogic Server is still
shutting down.>
```

Description and Solution

The error appears in the Administration Server log file due to unsuccessful lock cleanup. To fix this error, delete the `EmbeddedLDAP.lock` file (Located at, `ORACLE_BASE/admin/domain_name/aserver/domain_name/servers/AdminServer/data/ldap/ldapfiles/`).

Issue

The Administration Server might not start after performing switchover or failover operation. The Administration Server output log file reports the following error:

```
<Sep 16, 2011 2:04:06 PM PDT> <Error> <Store> <BEA-280061> <The persistent store
"_WLS_AdminServer" could not be deployed: weblogic.store.PersistentStoreException:
```

```
[Store:280105]The persistent file store "_WLS_AdminServer" cannot open file _WLS_
ADMINSERVER000000.DAT.>
```

Description and Solution

This error might appear due to the locks from Network File System (NFS) storage. You must clear the NFS locks using the NFS utility of the storage vendor. You may also copy the .DAT file to a temporary location, and copy it back, to clear the locks.

Issue

Some host on the new primary system might not be available, or might be down while performing switchover or failover operation. In such situations, Oracle Site Guard cannot perform any operation on these hosts.

Description and Solution

If the services running on these hosts are not mandatory, and the site can still be functional and active with the services running on the other nodes, the steps pertaining to the hosts, which are down, can be disabled by updating the operation plan. The Oracle Site Guard workflow skips all the disabled steps from the workflow.

Issue

If all the Oracle RAC Database instances are down, the switchover or failover operation fails.

Description and Solution

While creating an operation plan, Oracle Site Guard determines the Oracle RAC Database instance on which the switchover or failover operation is performed. RAC deployment can have multiple instances, and it is possible that some of the instances are down. Before running the switchover or failover operation, ensure that at least one of the instance is running. You can identify the name of the RAC instance, which is used by Oracle Site Guard to perform the role reversal operation, by running the `get_operation_plan_details` command.

E.5.3 Precheck Failure

This section provides tips for troubleshooting precheck failures.

Issue

Prechecks fail, displaying the following error:

```
Nmo setuid status NMO not setuid-root (Unix-only)
```

Description and Solution

After installing the Oracle Management Agent, ensure that you run the `root.sh` script from the Enterprise Manager Cloud host and all hosts managed by Enterprise Manager, as described in the section "After You Install" in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

Issue

If the Oracle Management Agent is down, prechecks hang while trying to run commands on the remote host.

Description and Solution

Ensure that all hosts involved in an operation are active, and all the configured scripts are available on remote hosts in the configured locations. If the Oracle Management Agent cannot be reached for some reason, then check the log files from the Enterprise Manager Cloud Control console. If you have identified the hosts that are down, skip the precheck operation on those hosts.

E.5.4 Oracle WebLogic Server Failure

This section provides troubleshooting tips for Oracle WebLogic Server failure issues.

Issue

Node Manager might fail to start due to an error, like the following:

```
<Sep 13, 2011 8:45:37 PM PDT> <Error> <NodeManager> <BEA-300033> <Could not execute command "getVersion" on the node manager. Reason: "Access to domain 'base_domain' for user 'weblogic' denied".>
```

Description and Solution

This problem might occur if you have changed the Node Manager credentials and then have not run `nmEnroll` to ensure that the correct Node Manager username and password is supplied to each managed server.

To ensure that the correct Node Manager username and password has been supplied, run `nmEnroll` using the following syntax:

```
nmEnroll(domain_directory, node_manager_home)
```

For example:

```
nmEnroll('C:/oracle/user_projects/domains/prod_domain',
'C:/oracle/wlserver_10.3/common/nodemanager')
```

Note: Restart Node Manager for the changes to take effect.

Issue

The managed server does not start due to a connection failure of the WLS Administration Server in Enterprise Manager Cloud Control.

Description and Solution

To start the managed server, Oracle Site Guard requires the Administration Server and the Node Manager. To start and stop managed servers successfully, ensure that the Administration Server is running.

Issue

Oracle Site Guard does not include the WebLogic Server instances that are migrated to a different host in the work flow.

Description and Solution

After you create the operation plan, Oracle Site Guard does not include the WebLogic Server instances involved in the operation plan that are migrated to different hosts, as a result of server migration.

After you complete the server migration, refresh the WebLogic Server farm target from the Enterprise Manager Cloud Control console, to uptake the latest target changes that have happened in the farm. This step is mandatory for Enterprise Manager to resume its farm monitoring capabilities after any changes in the farm like server migration happens. Once the farm target is refreshed, you need to recreate the Oracle Site Guard operation plans to include all of the farm targets in the Oracle Site Guard workflow.

Issue

While creating an operation plan, you might see an error, like the following:

```
oracle.sysman.ai.siteguard.model.common.exception.DAOException: For hostName:
[2606:b400:800:89:214:4fff:fe46:2d52] credential of type HOSTNORMAL does not
exist for siteName: System1
```

Description and Solution

If you do not configure the listen address for the WebLogic Server instances running on the hosts where multiple IP addresses are configured, WebLogic Server randomly picks up an IP address, and reports that as the listen address. This IP address might not be a valid one, and can prevent you from creating operation plans. To fix the issue, using the Admin Console, configure WebLogic Server properly, with a resolvable listen address. After configuring Oracle WebLogic Server, restart the server, and re-discovered it again from the Enterprise Manager Cloud Control. For more information about listen address configuration, refer to the *Oracle Fusion Middleware Disaster Recovery Guide*.

E.5.5 Database Failure

This section provides tips for troubleshooting issues related to database operation failure.

Issue

The prechecks or database switchover or database failover operations fail, and display the following error:

```
Database Status:
DGM-17016: failed to retrieve status for database "racs"
ORA-16713: the Data Guard broker command timed out
```

Description and Solution

This error might occur if the Data Guard Monitor process (DMON) in the target database instance, is down.

Note: The Data Guard Monitor process (DMON) is part of the Oracle Data Guard Broker.

If this error occurs, restart the database instance, and ensure that the DMON process is running. You can also see the database log file for DMON-process errors. Use the `CommunicationTimeout` parameter to select an appropriate timeout value for the environment. For more information, see "CommunicationTimeout" in *Oracle Data Guard Broker*.

E.6 Frequently Asked Questions on Linux Provisioning

What is PXE (Pre-boot Execution Environment)?

The Pre-boot Execution Environment (PXE, aka Pre-Execution Environment) is an environment to bootstrap computers using a network interface card independently of available data storage devices (like hard disks) or installed operating systems. Refer to [Appendix D, "Understanding PXE Booting and Kickstart Technology"](#) for more information.

Can my boot server reside on a subnet other than the one on which the bare metal boxes will be added?

Yes. But it is a recommended best practice to have boot server in the same subnet on which the bare metal boxes will be added. If the network is subdivided into multiple virtual networks, and there is a separate DHCP/PXE boot server in each network, the Assignment must specify the boot server on the same network as the designated hardware server.

If one wants to use a boot server in a remote subnet then one of the following should be done:

-- Router should be configured to forward DHCP traffic to a DHCP server on a remote subnet. This traffic is broadcast traffic and routers do not normally forward broadcast traffic unless configured to do so. A network router can be a hardware-based router, such as those manufactured by the Cisco Corporation or software-based such as Microsoft's Routing and Remote Access Services (RRAS). In either case, you need to configure the router to relay DHCP traffic to designated DHCP servers.

-- If routers cannot be used for DHCP/BOOTP relay, set up a DHCP/BOOTP relay agent on one machine in each subnet. The DHCP/BOOTP relay agent relays DHCP and BOOTP message traffic between the DHCP-enabled clients on the local network and a remote DHCP server located on another physical network by using the IP address of the remote DHCP server.

Why is Agent rpm staged on the Stage server?

Agent rpm is used for installing the agent on the target machine after booting over the network using PXE. With operating system provisioning, agent bits are also pushed on the machine from the staging location specified in the Advanced Properties.

Can I use the Agent rpm for installing Agent on Stage and Boot Server?

This is true only if the operating system of the Stage or Boot Server machine is RedHat Linux 4.0, 3.1 or 3.0 or Oracle Linux 4.0 or later. Refer to section **Using agent rpm for Oracle Management Agent Installation** on the following page for more information:

http://www.oracle.com/technology/software/products/oem/htdocs/provisioning_agent.html

Can the yum repository be accessed by any protocol other than HTTP?

Though the rpm repository can be exposed via file:// or ftp:// as well, the recommended method is to expose it via http://. The latter is faster and more secure.

What is the significance of the Status of a directive? How can one change it?

Look at the following table to know the possible Status values and what they signify.

Table E-1 Status Values

Status	Description
Incomplete	This Status signifies that some step was not completed during the directive creation, for example uploading the actual script for the directive, or a user saved the directive while creating it and still some steps need to be performed to make complete the directive creation.
Ready	his signifies that the directive creation was successful and the directive is now ready to be used along with any component/image.
Active	A user can manually change the status of a Ready directive to Active to signify that it is ready for provisioning. Clicking Activate changes the Status to Active.

What is a Maturity Level of a directive? How can one change it?

See [Table E-2](#) to know the possible Status values and what they signify:

Table E-2 Maturity Levels

Maturity Level	Maturity Level Description
Untested	This signifies that the directive has not been tested and is the default maturity level that is assigned to the directive when it is created.
Beta	A directive can be manually promoted to Beta using the Promote button after testing the directive.
Production	A directive can be manually promoted to Production using the Promote button after a user is satisfied that the directive can be used for actual provisioning on production systems.

Can a same component be used in multiple deployments?

Yes. Components are reusable and a given component can be a part of multiple deployments at the same time.

Do I need to edit scheduled deployments associated with a component, if the component is edited?

Yes.

For creating the Linux OS component does the Reference Machine need to have a management agent running on it?

Yes. Reference Machine has to be one of the **managed targets** of the Enterprise Manager.

What is the significance of the Status of a component? How can one change it?

Status of a component is similar to that of a directive. Refer to [What is the significance of the Status of a directive? How can one change it?](#).

What is a Maturity Level of a component? How can one change it?

Maturity Level of a component is similar to that of a directive. Refer to [What is a Maturity Level of a directive? How can one change it?](#).

E.7 Refreshing Configurations

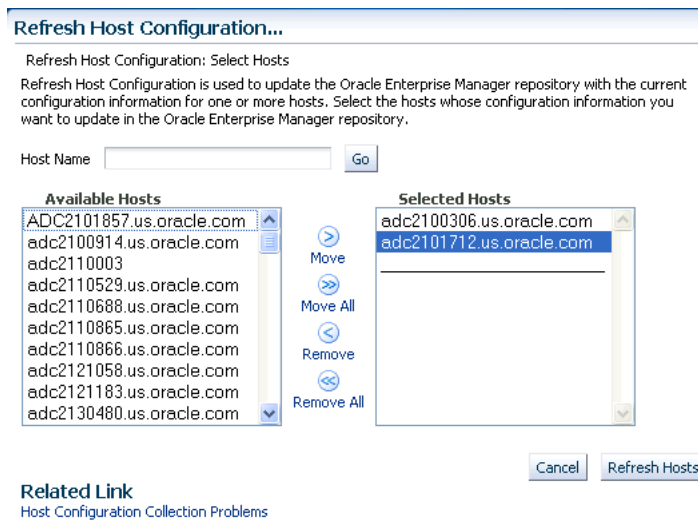
If you encounter issues and are expected to refresh the configurations in the host or the Oracle home, then follow the instructions outlined in the following sections:

- [Refreshing Host Configuration](#)
- [Refreshing Oracle Home Configuration](#)

E.7.1 Refreshing Host Configuration

Before you run any Deployment Procedure, Oracle recommends you to refresh the configuration of the hosts. To do so, follow these steps:

1. In Cloud Control, from the **Enterprise** menu, select **Configuration**, and then, click **Refresh Host Configuration**.
2. On the Refresh Host Configuration page, from the Available Hosts pane, select the hosts that the Deployment Procedure will use, and move them to the Selected Hosts pane.



3. Click **Refresh Hosts**.

E.7.2 Refreshing Oracle Home Configuration

Although the Oracle Management Agent running on a host automatically refreshes the host configuration information every 24 hours, you can also manually refresh the host configuration information the host.

Note: After patching the targets, refreshing the Oracle home configuration is handled internally by the deployment procedure. However if the refresh does not happen for some reason, then you can refresh the Oracle Home Configuration manually as described in this section.

To manually refresh the host configuration for one host:

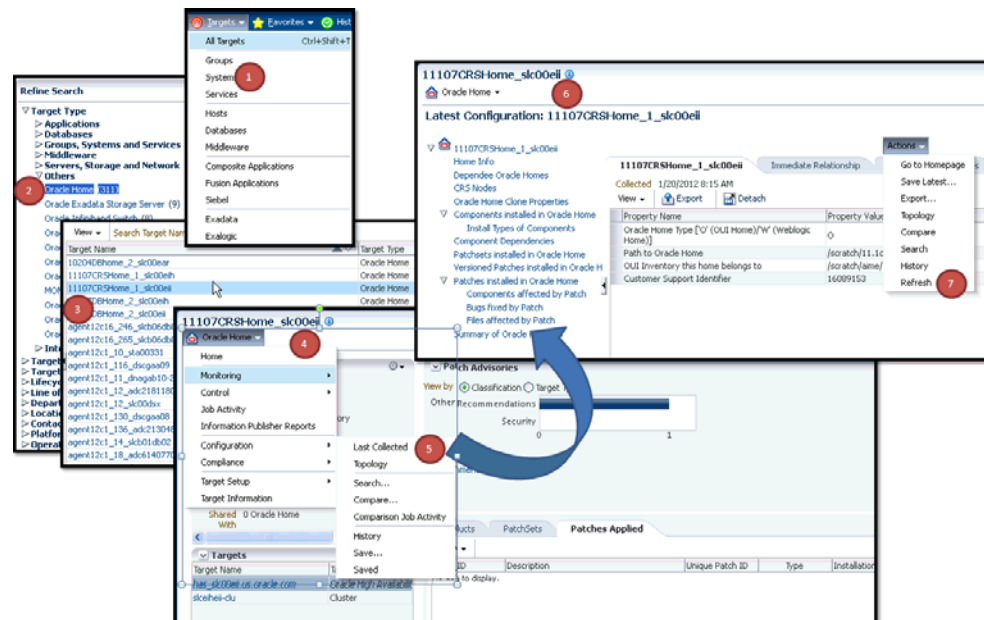
1. In Cloud Control, from the **Targets** menu, select **All Targets**.

- On the All Targets page, from the Refine Search section, click **Target Type** to expand the menu, and from the menu click **Others**, and then click **Oracle Home**.

On the right hand side of the page gets refreshed, and only the Oracle Home targets appear.

- Click the Target name to select it.
- On the <target_name> home page, from the **Oracle Home** menu, select **Configuration**, and then click **Last Collected**.
- On the latest Configuration:<target_name> page, from the **Actions** menu select **Refresh** to refresh the Oracle Home configuration for the host.

The following example describes the steps to refresh the Oracle home configuration for the target 11107CRSHome_1_slc00eii:



E.8 Reviewing Log Files

This section lists the log files you must review to resolve issues encountered while running a Deployment Procedure.

This section contains the following:

- [OMS-Related Log Files](#)
- [Management Agent-Related Log Files](#)
- [Advanced Options](#)

E.8.1 OMS-Related Log Files

The following are OMS-related log files.

Generic Enterprise Manager Trace File

```
<EM_INSTANCE_BASE>/em/<OMS_NAME>/sysman/log/emoms.trc
```

Generic Enterprise Manager Log File

```
<EM_INSTANCE_BASE>/em/<OMS_NAME>/sysman/log/emoms.log
```

Where, `<EM_INSTANCE_BASE>` is the OMS Instance Base directory. By default, the OMS Instance Base directory is `gc_inst`, which is present under the parent directory of the Oracle Middleware Home.

E.8.2 Management Agent-Related Log Files

The following are Management Agent-related log files:

```
EMSTATE/sysman/log/gcagent.log
```

```
EMSTATE/sysman/log/gcagent.trc
```

E.8.3 Advanced Options

Optionally, to capture more details, follow these steps to reset the log level and capture the logs mentioned in the previous sections.

Note: Oracle recommends you to archive the old logs and have a fresh run after resetting the log level to capture the fresh logs.

E.8.3.1 On the OMS Side

On the OMS side:

1. Open the following file available in the Oracle home of the OMS:
`$<ORACLE_HOME>/sysman/config/emomslogging.properties`
2. Set the `@log4j.category.oracle.sysman.emdrep.jobs =` parameter to `DEBUG`.

E.8.3.2 On the Management Agent Side

On the Management Agent side:

1. Open the following file:
`EMSTATE/sysman/config/emd.properties`
2. Make the following settings:
`Logger.log4j.rootCategory=DEBUG, Rolling, Errors`

Oracle Site Guard Command-Line Interface Reference

Oracle Site Guard uses the Enterprise Manager Command Line Interface (EMCLI) to manage Oracle Site Guard configuration directly from the command line, or from batch programs or scripts.

Note: EMCLI commands are case-sensitive. Ensure that you use the correct EMCLI verb, and enter the correct input.

This chapter lists all of the EM CLI verbs used for configuring Oracle Site Guard:

- `add_siteguard_script_hosts`
- `create_operation_plan`
- `create_siteguard_configuration`
- `create_siteguard_credential_association`
- `create_siteguard_script`
- `delete_operation_plan`
- `delete_siteguard_configuration`
- `delete_siteguard_credential_association`
- `delete_siteguard_script`
- `delete_siteguard_script_hosts`
- `get_operation_plan_details`
- `get_operation_plans`
- `get_siteguard_configuration`
- `get_siteguard_credential_association`
- `get_siteguard_script_hosts`
- `get_siteguard_scripts`
- `run_prechecks`
- `submit_operation_plan`
- `update_operation_plan`
- `update_siteguard_configuration`

- [update_siteguard_credential_association](#)
- [update_siteguard_script](#)

See: For more information about EMCLI, see *Oracle Enterprise Manager Command Line Interface*.

F.1 add_siteguard_script_hosts

Adds a host to the Oracle Site Guard configuration scripts. You can add more than one host.

Format

```
emcli add_siteguard_script_hosts
      -script_id="script_id"
      -host_name="name1;name2;..."
```

Parameter	Description
-script_id	Specify the identification associated with the script.
-host_name	Specify the host that you want to associate with the script. You can specify more than one host name.

Example F-1 Adding Hosts

```
emcli add_siteguard_script_hosts
      -script_id="10"
      -host_name = "BIHOST1;BIHOST2"
```

F.2 create_operation_plan

Creates an operational plan for Oracle Site Guard operations.

Format

```
emcli create_operation_plan
      -primary_system_name="name"
      -standby_system_name="name"
      -system_name="name"
      -operation="name"
      -name="name"
      -role="role"
```

Parameter	Description
-primary_system_name	Specify the name of your system associated with the primary site. Enter this option for switchover or failover operations.
-standby_system_name	Specify the name of your system associated with the standby site. Enter this option for switchover or failover operations.
-system_name	Specify the name of the system. Enter this option for start or stop operations.
-operation	Specify the function of the operation. Example: switchover, failover, start or stop.
-name	Specify the name of the operation plan.

Parameter	Description
-role	Specify the role associated with a system, when you run an operation (start or stop).

Example F-2 Creating Operation Plan

```
emcli create_operation_plan
  -primary_system_name="BISystem1"
  -standby_system_name="BISystem2"
  -operation="switchover"
  -name="BISystem1-switchover-plan"

emcli create_operation_plan
  -system_name="austin"
  -operation="start"
  -name="BISystem1-start-plan"
  -role="Primary"
```

F.3 create_siteguard_configuration

Creates a site configuration for Oracle Site Guard. It associates the systems and their roles.

Format

```
emcli create_siteguard_configuration
  -primary_system_name="name"
  -standby_system_name="name1;name2;..."
```

Parameter	Description
-primary_system_name	Specify the name of the system that is associated with the primary site.
-standby_system_name	Specify the name of the system that is associated with the standby system. You can specify more than one option and one system name.

Example F-3 Creating Site Guard Configuration

```
emcli create_siteguard_configuration
  -primary_system_name="BISystem1"
  -standby_system_name="BISystem2"
```

F.4 create_siteguard_credential_association

Associates the credentials with the targets in a site.

Format

```
emcli create_siteguard_credential_association
  -system_name="name"
  [-target_name="name"]
  -credential_type="type"
  [-credential_name="name"]
  -credential_owner="owner"
  [-use_preferred_credential="true_or_false"]
```

Note: [] indicates that the parameter is optional.

Parameter	Description
-system_name	Specify the name of the system.
-target_name	Specify the name of the target. This parameter is optional.
-credential_type	Specify the type of the credential. Example: HostNormal, HostPrivileged, WLSAdmin, or DatabaseSysdba.
-credential_name	Specify the name of the credential.
-credential_owner	Specify the owner of the credential.
-use_preferred_credential	If you are using Preferred Credentials, then specify true. The default value is false. If you use the default value, then you must specify the -credential_name parameter to use named credentials.

Example F-4 Creating Site Guard Credential Association

```
emcli create_siteguard_credential_association
  -system_name="BISystem1"
  -credential_type="HostNormal"
  -credential_name="HOST-SGCREd"
  -credential_owner="sysman"
  -use_preferred_credential="false"
```

```
emcli create_siteguard_credential_association
  -system_name="BIsystem1"
  -target_name="database-instance"
  -credential_type="HostNormal"
  -credential_name="HOST-DBCRED"
  -credential_owner="sysman"
  -use_preferred_credential="false"
```

```
emcli create_siteguard_credential_association
  -system_name="BISystem1"
  -credential_type="HostNormal"
  -credential_owner="sysman"
  -use_preferred_credential="true"
```

F.5 create_siteguard_script

Associates scripts (pre-script, post script and storage script) with the Oracle Site Guard configuration.

Format

```
emcli create_siteguard_script
  -system_name="name"
  -operation="name"
  -script_type="type"
  [-host_name="name1;name2;..."]
  -path="path"
```

```
[-all_hosts="true_or_false"]
-credential_type="type"
[-role="role"]
```

Note: [] indicates that the parameter is optional.

Parameter	Description
-system_name	Specify the name of the system.
-operation	Specify the name of the operation. For example: Switchover, Failover, Start, or Stop.
-script_type	Specify the type of the script. It can be Mount, UnMount, Pre-Script, Post-Script, Failover, or Switchover.
-host_name	Specify the name of the host where this script will be executed. This parameter is optional and can be specified more than once.
-path	Specify the path to the script.
-all_hosts	Optional flag to allow the script to run on all the hosts in the system. This parameter overrides the host_name. For example: true or false.
-credential_type	Specify HostNormal or HostPrivileged if you have the root privileges.
-role	Optional flag to configure script based on the system role. By default, the script is configured for both primary and standby roles for a given system. For example: Primary or Standby.

Example F-5 Creating Site Guard Script

```
emcli create_siteguard_script
  -system_name="BISystem1"
  -operation="Switchover"
  -script_type="Pre-Script"
  -path="/tmp/prescript"
  -all_hosts="true"
  -credential_type="HostNormal"
  -role="Primary"

emcli create_siteguard_script
  -system_name="BISystem1"
  -operation="Switchover"
  -script_type="Pre-Script"
  -path="/tmp/prescript"
  -credential_type="HostNormal"
  -host_name="BIHOST1"
  -host_name="BIHOST2"
```

F.6 delete_operation_plan

Deletes the specified operation plan from a Site Guard configuration.

Format

```
emcli delete_operation_plan
    -name="plan_name"
```

Parameter	Description
-name	Specify the name of the operation plan you want to delete.

Example F-6 Deleting the Operation Plan

```
emcli delete_operation_plan
    -name="BISystem1-switchover"
```

F.7 delete_siteguard_configuration

Deletes the Oracle Site Guard configuration. The entire configuration (scripts, credential associations, site associations, operation plans) pertaining to the specified system and all of the associated standby systems, are deleted.

Format

```
emcli delete_siteguard_configuration
    -primary_system_name="name"
    [-standby_system_name="name"]
```

Note: [] indicates that the parameter is optional.

Parameter	Description
-primary_system_name	Specify the name of the primary system. Specify either <code>primary_system_name</code> or <code>standby_system_name</code> .
-standby_system_name	Specify the name of the standby system. This parameter is optional. However, if you do not specify this parameter, the Oracle Site Guard configuration of the specified primary system and all its standby system are deleted.

Example F-7 Deleting Site Guard Configuration

```
emcli delete_siteguard_configuration
    -primary_system_name="BISystem1"

emcli delete_siteguard_configuration
    -standby_system_name="BISystem2"
```

F.8 delete_siteguard_credential_association

Deletes the credential association from the Oracle Site Guard configuration.

Format

```
emcli delete_siteguard_credential_association
    -system_name="name"
```

```
[-target_name=["name"]]
-credential_type="type"
```

Note: [] indicates that the parameter is optional.

Parameter	Description
-system_name	Specify the system on which the service resides.
-credential_type	Specify the credential type. It can be HostNormal, HostPrivileged, WLSAdmin, or DatabaseSysdba.
-target_name	Specify the name of the target. This parameter is optional.

Example F-8 Deleting Site Guard Credential Association

```
emcli delete_siteguard_credential_association
  -system_name="BISystem1"
  -credential_type="HostNormal"
```

```
emcli delete_siteguard_credential_association
  -system_name="BISystem2"
  -target_name="austin-database-instance"
  -credential_type="HostNormal"
```

F.9 delete_siteguard_script

Deletes the specified script from the Oracle Site Guard configuration.

Format

```
emcli delete_siteguard_script
  -script_id="script id"
```

Parameter	Description
-script_id	Specify the ID associated with the script.

Example F-9 Deleting Site Guard Script

```
emcli delete_siteguard_script
  -script_id="10"
```

F.10 delete_siteguard_script_hosts

Deletes the host or hosts associated with a given script.

Format

```
emcli delete_siteguard_script_hosts
  -script_id="script id"
  -host_name="name1;name2;..."
```

Parameter	Description
-script_id	Specify the ID associated with the script.
-host_name	Specify the name of the host where this script will be executed. This parameter can be specified more than once.

Example F-10 Deleting Site Guard Script Hosts

```
emcli delete_siteguard_script_hosts
      -script_id="10"
      -host_name="BIHOST1"
```

F.11 get_operation_plan_details

Provides the detailed step-by-step information about the specified operation plan.

Format

```
emcli get_operation_plan_details
      -name="plan name"
```

Parameter	Description
-name	Specify the name of the operation plan.

Example F-11 Obtaining Operation Plan Details

```
emcli get_operation_plan_details
      -name="BISystem1-switchover"
```

F.12 get_operation_plans

Lists all configured operation plans.

Format

```
emcli get_operation_plans
      [-name="operation_plan_name"]
      [-operation="operation_name"]
```

Note: [] indicates that the parameter is optional.

Parameter	Description
-name	Specify the name of the operation plan.
-operation	Specify the name of the operation. For example, switchover, failover, start, or stop. This is an optional parameter. If you do not specify this parameter, then all the operation plans will be listed.

Example F-12 Obtaining Operation Plans

```
emcli get_operation_plans
      -name="austin-switchover"
      -operation="switchover"
```

F.13 get_siteguard_configuration

Provides the Oracle Site Guard configuration.

Format

```
emcli get_siteguard_configuration
      [-primary_system_name="name_of_the_primary_system"]
      [-standby_system_name="name_of_the_standby_system"]
```

Note: [] indicates that the parameter is optional.

Parameter	Description
-primary_system_name	Specify the name of the primary system.
-standby_system_name	Specify the name of the standby system.

Example F-13 Obtaining Site Guard Configuration

```
emcli get_siteguard_configuration
      -primary_system_name="BISystem1"
      -standby_system_name="BISystem2"
```

F.14 get_siteguard_credential_association

Lists the credential associations configured for a system.

Format

```
emcli get_siteguard_credential_association
      -system_name="name_of_the_system"
      [-target_name="name_of_the_target"]
      [-credential_type="type_of_the_credential"]
```

Note: [] indicates that the parameter is optional.

Parameter	Description
-system_name	Specify the name of the system.
-target_name	Specify the name of the target. This parameter is optional.
-credential_type	Specify the type of the credential. It can be HostNormal, HostPrivileged, WLSAdmin, or DatabaseSysdba. This parameter is optional.

Example F-14 Obtaining Site Guard Credential Association

```
emcli get_siteguard_credential_association
    -system_name="BISystem1"
    -credential_type="HostNormal"

emcli create_siteguard_credential_association
    -system_name="BISystem1"
    -target_name="BI-database-instance"
    -credential_type="HostNormal"
```

F.15 get_siteguard_script_hosts

Lists the hosts associated with any script where the script is designated to run.

Format

```
emcli get_siteguard_script_hosts
    -script_id="script_id"
```

Parameter	Description
-script_id	Specify the ID associated with the script.

Example F-15 Obtaining Site Guard Script Hosts

```
emcli get_siteguard_script_hosts
    -script_id="10"
```

F.16 get_siteguard_scripts

Obtains the Oracle Site Guard scripts associated with the specified system.

Format

```
emcli get_siteguard_scripts
    -system_name="system_name"
    -operation="operation_name"
    [-script_type="type_of_the_script"]
    [-role="role_of_the_system"]
```

Note: [] indicates that the parameter is optional.

Parameter	Description
-system_name	Specify the name of the system.
-operation	Specify the name of the operation. For example, switchover, failover, start, or stop.
-script_type	Specify the type of the script. For example: mount, unmount, pre-script, post-script, failover, or switchover.
-role	Optional parameter to filter the scripts based on the role associated with the system. For example: Primary or Standby.

Example F-16 Obtaining Site Guard Scripts

```
emcli get_siteguard_scripts
  -system_name="BISystem1"
  -operation="Switchover"
  -script_type="Pre-Script"

emcli get_siteguard_scripts
  -system_name="BISystem2"
  -operation="Switchover"
  -script_type="Pre-Script"
  -role="Primary"
```

F.17 run_prechecks

Submits the prechecks for any given operation plan.

Format

```
emcli run_prechecks
  -operation_plan="name_operation plan"
```

Parameter	Description
-operation_plan	Specify the name of the operation plan.

Example F-17 Running Prechecks

```
emcli run_prechecks
  -operation_plan="BISystem1-switchover"
```

F.18 submit_operation_plan

Submits the specified operation plan for execution.

Format

```
emcli submit_operation_plan
  -name="name_operation plan"
  [-run_prechecks="true_or_false"]
```

Note: [] indicates that the parameter is optional.

Parameter	Description
-name	Specify the name of the operation plan.
-run_prechecks	Specify the run_prechecks value (true or false). By default, the value of this parameter is true. If you set the value to false, prechecks will not be executed.

Example F-18 Submitting Operation Plan

```
emcli submit_operation_plan
  -name="austin-switchover"
```

F.19 update_operation_plan

Updates the Error Mode and Run Mode for any step in the given operation plan.

Format

```
emcli update_operation_plan
      -name="operation_plan_name"
      [-step_number="step_number"]
      [-target_host="host_name"]
      [error_mode="error_mode"]
      [enabled="true_or_false"]
      [-execution_mode="Serial_or_Parallel"]
      [-move="Up_or_Down"]
```

Note: [] indicates that the parameter is optional.

Parameter	Description
-name	Specify the name of the operation plan.
-step_number	Specify the number of the step that should be updated.
-target_host	Specify the name of the system. Enter this option for starting or stopping operation.
-error_mode	The function of the operation. For example: stop or continue.
-enabled	Enter true or false.
-execution_mode	Specify the execution mode. For example: Serial or Parallel
-move	Change the order by specifying Up or Down.

Example F-19 Updating an Operation Plan

```
emcli update_operation_plan
      -name="austin-switchover"
      -step_number="1"
      -error_mode="Continue"
      -enabled="true"
      -execution_mode="Serial"

emcli update_operation_plan
      -name="austin-switchover"
      -target_host="myhost.domain.com"
      -error_mode="Continue"
      -enabled="true"

emcli update_operation_plan
      -name="austin-switchover"
      -step_number="5"
      -move="Up"
```

F.20 update_siteguard_configuration

Updates the Oracle Site Guard configuration to add additional standby systems. One primary system can be associated with one or more standby systems.

Format

```
emcli update_siteguard_configuration
    -primary_system_name="primary_system_name"
    -standby_system_name="standby_system_name"
```

Parameter	Description
-primary_system_name	Specify the name of the primary system.
-standby_system_name	Specify the name of the standby system. This parameter can be specified more than once.

Example F-20 Updating Site Guard Configuration

```
emcli update_siteguard_configuration
    -primary_system_name="BISystem1"
    -standby_system_name="BISystem2"
```

Note: If you update the site configuration, then you must update the operation plan, as described in [update_operation_plan](#).

F.21 update_siteguard_credential_association

Updates the credential association.

Format

```
emcli update_siteguard_credential_association
    -system_name="name_of_the_system"
    [-target_name="name_of_the_target"]
    -credential_type="type_of_the_credential"
    [-credential_name="name_of_the_credential"]
    -credential_owner="credential_owner"
    [-use_preferred_credential="true_or_false"]
```

Note: [] indicates that the parameter is optional.

Parameter	Description
-system_name	Specify the name of the system.
-target_name	Specify the name of the target. This parameter is optional.
-credential_type	Specify the type of the credential. It can be HostNormal, HostPrivileged, WLSAdmin, or DatabaseSysdba.
-credential_name	Specify the name of the credential.
-credential_owner	Specify the owner of the credential.
-use_preferred_credential	If you are using Preferred Credentials, then specify true. The default value is false. If you specify the default value, then you must specify the -credential_name parameter to use named credentials.

Example F-21 Updating Site Guard Credential Association

```
emcli update_siteguard_credential_association
  -system_name="austin-system"
  -credential_type="HostNormal"
  -credential_name="HOST-SGCREd"
  -credential_owner="sysman"

emcli update_siteguard_credential_association
  -system_name="austin-system"
  -target_name="austin-database-instance"
  -credential_type="HostNormal"
  -credential_name="HOST-DBCRED"
  -credential_owner="sysman"

emcli update_siteguard_credential_association
  -system_name="austin-system"
  -target_name="austin-database-instance"
  -credential_type="HostNormal"
  -credential_owner="sysman"
  -use_preferred_credential="true"
```

F.22 update_siteguard_script

Updates the path and the all_hosts flag associated with any script.

Format

```
emcli update_siteguard_script
  -script_id="ID_associated_with_the_script"
  [-path="path_of_the_script"]
  -credential_type="type"
  [-all_hosts="true_or_false"]
```

Note: [] indicates that the parameter is optional.

Parameter	Description
-script_id	Specify the script ID.
-path	Specify the path to the script.
-credential_type	Specify HostNormal or HostPrivileged if you have the root privileges.
-all_hosts	Optional flag to allow the script to run on all the hosts in the system. For example: true or false.

Example F-22 Updating Site Guard Script

```
emcli update_siteguard_script
  -script_id="10"
  -path="/tmp/newprescript"
  -credential_type="HostNormal"
  -all_hosts="true"
```

A

accessing Software Library console, 2-2
adding
 component step, 33-6
 directive step, 33-5
 file transfer step, 33-7
 host command step, 33-7
 job step, 33-4
 manual step, 33-8
adding new target data collections, 26-42
Adding phases
 rolling and parallel, 33-3
AIX Installed Packages parser, 26-54
analyzing configuration health, 26-71
AND/OR logical operators
 in comparison rules, 26-24
Apache HTTPD parser, 26-54
associations. See relationships
Autosys parser, 26-54

B

bare metal provisioning
 concepts
 boot server, 23-2
 reference host, 23-3
 RPM repository, 23-3
 stage server, 23-3
 overview, 23-2
 process, 23-3
 setting up, 23-4
 supported releases, 23-4
base parsers
 columnar, 26-52
 format-specific, 26-48
 properties, 26-54
BEA Tuxedo parser. See Ubb Config parser
Blue Martini DNA parser, 26-48
blueprints, for custom configurations, 26-43
boot server, 23-2
 overview, 23-2
 setting up, 23-5
Business Process Execution Language (BPEL), 21-1

C

change management, 28-1
change plans
 overview, 28-23
 setting up, 28-28
Client Configuration Collection Tag, 26-67
client configurations, 26-66
Client System Analyzer (CSA)
 client configurations, 26-66
 deployed independently, 26-67
clone
 cloning a running Oracle Application Server instance, 22-2
 cloning a running Oracle database replay client, 12-2
 cloning a running Oracle RAC instance, 9-2
Cloning a Middleware Home from an Existing Installation
 Prerequisites, 15-18
 Provisioning Procedure, 15-19
Cloning a WebLogic Domain From an Existing Installation
 Prerequisites, 15-11
Cloning From a WebLogic Domain Provisioning Profile
 Prerequisites, 15-21
Cloning From an Existing Installation
 Provisioning Procedure, 15-11
Cloning from an Oracle Middleware Home Gold Image
 Prerequisites, 15-23
 Provisioning Procedure, 15-23
Coherence Node Provisioning
 Deploying Coherence Nodes and Clusters, 18-2
 Getting Started, 18-1
collected configurations for targets, 26-1
columnar
 parser parameters, 26-53
 parsers, 26-52
comparing configurations, 26-25
comparing data, 28-31
comparison
 rules, 1-3
comparison job activity, 26-28
comparison template

- creating or editing, 26-16
 - deleting, 26-18
 - exporting, 26-18
 - importing, 26-18
 - managing, 26-17, 26-37
 - Member Settings tab, 26-16
 - Property Settings tab, 26-17
 - Rules for Ignoring tab, 26-17
 - Rules for Matching tab, 26-17
 - Template Settings tab, 26-16
 - viewing, 26-18
- comparison wizard, 26-25
- compliance
 - accessing, 27-4
 - compliance frameworks, 27-24
 - compliance standard rule folders, 27-43
 - compliance standard rules, 27-44
 - compliance standards, 27-32
 - evaluating, 27-5
 - importance, 27-16
 - investigating evaluation errors, 27-14
 - managing, 27-23
 - overview, 27-1
 - privileges needed to use, 27-4
 - real-time monitoring facets, 27-61
 - reports, 27-15
 - roles needed to use, 27-4
 - score, 27-16
 - terminology used in, 27-2
- compliance frameworks
 - about, 27-24
 - accessing, 27-24
 - adding compliance standard to, 27-27
 - benefits of using, 27-25
 - browsing, 27-30
 - compliance of database targets, 27-32
 - compliance score, 27-18
 - creating, 27-26
 - creating like, 27-28
 - deleting, 27-29
 - editing, 27-28
 - editing importance, 27-27
 - errors, 27-31
 - evaluation results, 27-30, 27-31
 - exporting, 27-29
 - importing, 27-30
 - operations on, 27-26
 - provided by Oracle, 27-24
 - reasons for using, 27-25
 - searching, 27-30
- compliance score
 - compliance framework, 27-18
 - compliance standard for a target, 27-17
 - compliance standard rule-target, 27-16
 - parent node, 27-18
 - real-time monitoring rule, 27-17
- compliance standard rule folders
 - about, 27-43
 - creating, 27-43
 - managing in compliance standard, 27-44
- compliance standard rules
 - about, 27-44
 - browsing, 27-60
 - creating, 27-45
 - creating like, 27-58
 - deleting, 27-59
 - editing, 27-58
 - exporting, 27-59
 - importance, 27-45
 - importing, 27-60
 - operations on, 27-45
 - provided by Oracle, 27-60
 - real-time monitoring rules, 27-45
 - repository rules, 27-44
 - searching, 27-60
 - types, 27-44
 - WebLogic Server Signature rules, 27-44
- compliance standards
 - about, 27-32
 - accessing, 27-33
 - adding to another compliance standard, 27-36
 - associating with targets, 27-41
 - browsing, 27-39
 - creating, 27-35
 - creating like, 27-37
 - customizing, 27-37
 - deleting, 27-38
 - editing, 27-37
 - errors, 27-40
 - evaluation results, 27-39, 27-40
 - exporting, 27-38
 - importing, 27-38
 - investigating violations, 27-10
 - operations on, 27-34
 - searching, 27-39
 - security metrics, enabling, 27-42
- compliance violations, investigating, 27-10
- Configuration Browser, viewing
 - configurations, 26-7
- configuration changes, 26-11
- configuration comparison
 - add configurations, 26-26
 - first configuration, 26-25
 - ignore rule, 26-20
 - ignore rule example, 26-23
 - key properties, 26-31
 - matching rule, 26-19
 - matching rule example, 26-22
 - resubmit, 26-28
 - results, 26-28
 - review and submit, 26-27
 - rule examples, 26-22
 - rule language, 26-20
 - rules, 26-19
 - schedule and notify, 26-27
 - selecting template, 26-26
 - single target results, 26-29
 - system results, 26-29
 - value constraint rule, 26-19
 - wizard, 26-25

- configuration data, extending collections, 26-41
- configuration history, job activity, 26-15
- configuration searches
 - creating, 26-4
 - options, 26-5
 - scenarios, 26-6
 - SQL queries, 26-5
- Configuration Topology Viewer, 26-69
- configuration topology, viewing, 26-70
- configurations
 - client, 26-66
 - Client System Analyzer (CSA), 26-66
 - hardware and software, 26-1
 - history, 1-3
 - searching, 1-3, 26-3
 - viewing, 26-7
- configure Grid Infrastructure, 7-6, 7-18
- Connect:Direct parser, 26-48
- controlling appearance of information on a graph, 26-76
- copying customized provisioning entities., 33-15
- creating
 - comparison template, 26-16
 - configuration search, 26-4
 - custom target type, 26-33
 - new relationships, 26-68
- creating a change plan, 28-25
- creating change plans using external clients, 28-27
- creating database provisioning entities, 4-14
- creating database templates, 4-12
- creating databases, 7-20
- creating Disk Layout component, 23-14
- creating installation media, 4-10
- creating Oracle Database, 13-2
 - prerequisites, 13-2
 - procedure, 13-2
- creating Oracle RAC One Node Database, 13-8
 - prerequisites, 13-8
 - procedure, 13-9
- creating Oracle Real Application Clusters Database, 13-5
 - prerequisites, 13-5
 - procedure, 13-6
- creating provisioning profiles, 4-9
- creating relationships to a target, 26-75
- Creating Software Library Components
 - Creating a WebLogic Domain Provisioning Profile, 15-6
 - Creating an Oracle Middleware Home Gold Image, 15-8
- creating users
 - designers, 2-18
 - operators, 2-19
- credentials, for custom configurations, 26-36
- Cron Access parser, 26-52
- Cron Directory parser, 26-52
- CSV parser, 26-52
- Custom CFG parser, 26-54
- custom configuration
 - blueprints, 26-43
 - creating, 26-33
 - credentials, 26-36
 - custom target type, 26-33
 - database roles, 26-35
 - deleting, 26-38
 - deploying, 26-40
 - editing, 26-33
 - editing deployment, 26-41
 - enabling facet synchronization, 26-37
 - encoding, 26-34
 - exporting, 26-38
 - Files & Commands tab, 26-34
 - importing, 26-38
 - post-parsing rule, 26-62, 26-64, 26-66
 - privileges, 26-39
 - roles, 26-39
 - rules, 26-36
 - sample non-XML parsed file, 26-63
 - sample parsed SQL query, 26-65
 - sample XML parsed file, 26-62
 - undeploying, 26-40
 - versioning, 26-38
 - viewing collection data, 26-41
 - viewing specification details, 26-37
 - XML parsed example (default), 26-47
 - XML parsed example (generic), 26-48
 - XML parsed example (modified), 26-48
 - XPath, 26-36
- customization
 - changing error handling modes, 33-11
 - customization types, 33-1
 - directive workflow, 33-15
 - editing deployment procedure, 33-10
 - overview, 33-1
 - phases or steps
 - adding phases or steps, 33-3
 - deleting, 33-9
 - enabling or disabling, 33-10
 - setting up e-mail notifications, 33-12
- customizing compliance standards, 27-37
- customizing topology views, 26-73

D

- data comparison, 28-2
 - overview, 28-29
- database credentials, 26-35
- database host readiness, B-1
 - adding user accounts, B-1
 - configuring SSH, B-2
 - environment settings, B-2
 - kernel requirements, B-3
 - memory requirements, B-4
 - network and IP requirements, B-4
 - node time requirements, B-3
 - package requirements, B-4
- installation directories and Oracle inventory, B-6
- PDP setup, B-2
- setting user accounts, B-1
- shell limits, B-2

- storage requirements, B-5
- database provisioning
 - administrator privileges, 4-6
 - deployment procedures, 4-3
 - getting started, 5-1
 - host requirements, 4-6
 - Oracle Database software, 5-13
 - Oracle Databases with Oracle ASM, 5-8
 - Oracle Grid Infrastructure and Oracle Database software, 6-7
 - Oracle Grid Infrastructure and Oracle Databases with Oracle ASM, 6-2
 - Oracle Grid Infrastructure for Oracle Real Application Clusters Databases, 7-1
 - Oracle RAC database with file system on existing cluster, 7-11
 - Oracle RAC database with file system on new cluster, 7-16
 - Oracle Real Application Clusters One Node databases, 8-1
 - prerequisites for designers, 4-7
 - prerequisites for operators, 4-8
 - provisioning and creating Oracle Databases, 5-3
 - provisioning Oracle RAC, 9-1
 - setup, 4-5
 - supported targets, 4-3
 - usecases, 4-4
- database provisioning overview, 4-1
- database provisioning solution
 - accessing the screen, 4-2
- Database Query
 - parser, 26-48
 - parser parameters, 26-49
- Db2 parser, 26-48
- delete Oracle RAC, 11-2
 - prerequisites, 11-2
- delete Oracle RAC nodes, 11-5
- deleting
 - comparison template, 26-18
 - custom configuration, 26-38
 - custom topology views, 26-74
 - relationships from a target, 26-75
- dependency analysis, 26-73
- deployable patch plan, 24-5
- Deploying Coherence Nodes and Clusters
 - Creating a Coherence Component, 18-3
 - Deployment Procedure, 18-4
 - Prerequisites, 18-2
 - Troubleshooting, 18-16
- deploying custom configurations, 26-40
- deploying SOA composites, 19-8
- Deploying, Undeploying or Redeploying Java EE Applications
 - Creating a Java EE Application Component, 17-3
 - Deploying a Java EE Application, 17-4
 - Getting Started, 17-1
 - Java EE Applications Deployment Procedure, 17-4
 - Prerequisites, 17-2
 - Redeploying a Java EE Application, 17-8

- Undeploying a Java EE Application, 17-10
- Deploying, Undeploying, or Redeploying Java EE Applications, 17-1
- deployment procedures
 - editing the permissions, 32-22
 - phases and steps, 32-10
 - target list, 32-9
 - tracking the status, 32-22
 - User, roles and privileges, 32-6
 - variables, 32-9
 - viewing, editing, and deleting, 32-22
- deployments
 - Client Configuration Collection Tag, 26-67
 - Client System Analyzer (CSA), 26-67
 - Management Repository, 26-1
- Designer and Operator Roles, 4-2
- determining configuration health compliance score, 26-72
- dhcp server
 - setting up, 23-5
- diagnosing
 - compliance violations, 27-10
- Directory
 - parser, 26-48
 - parser parameters, 26-50
- Disaster Recovery
 - key aspects, 30-5
- discovering hosts, 3-1
 - automatically, 3-1
 - manually, 3-1

E

- E-Business Suite
 - parser, 26-49
 - parser parameters, 26-50
- editing
 - comparison template, 26-16
 - custom configuration deployment, 26-41
- EM_ALL_DESIGNER
 - EM_PATCH_DESIGNER, 32-7
 - EM_PROVISIONING_DESIGNER, 32-7
 - EM_TC_DESIGNER, 32-7
- EM_ALL_OPERATOR
 - EM_ALL_VIEWER, 32-7
 - EM_HOST_DISCOVERY_OPERATOR, 32-7
 - EM_PATCH_OPERATOR, 32-7
 - EM_PROVISIONING_OPERATOR, 32-7
 - EM_TARGET_DISCOVERY_OPERATOR, 32-7
- EM_COMPLIANCE_DESIGNER role, 26-39
- EM_PLUGIN_AGENT_ADMIN role, 26-39
- EM_PLUGIN_OMS_ADMIN role, 26-39
- e-mail notifications
 - configuring outgoing mail server, 33-12
 - entering administrator e-mail and password, 33-14
 - overview, 2-20
- EMCLI, A-1
 - advantages, A-1
 - creating properties file, A-12

- launching a procedure with an existing saved procedure, A-16
- limitations, A-40
- overview, A-1
- prerequisites, A-2
- provisioning Oracle WebLogic Server
 - using provisioning profile, A-26
- provisioning Oracle Database software, A-25
- provisioning Oracle WebLogic Server, A-26
 - scaling up or scaling out, A-29
- provisioning user defined deployment procedure, A-30
 - adding steps/phases, A-31
 - prerequisites, A-31
 - running the procedure, A-32
- using an existing properties file, A-15
- verbs, A-2
 - deployment procedure verbs, A-3
 - new deployment procedure verbs, A-2
 - old deployment procedure verbs, A-3
- EMCLI verbs
 - confirm_instance, A-3, A-6
 - describe_instance, A-4, A-6
 - describe_procedure_input, A-2, A-4
 - get_executions, A-2, A-4, A-6
 - get_instance_data, A-2, A-4, A-6
 - get_instance_status, A-4, A-7
 - get_instances, A-4, A-6
 - get_procedure_types, A-4, A-7
 - get_procedure_xml, A-4, A-7
 - get_procedures, A-4, A-7
 - get_retry_argument, A-4, A-7
 - ignore_instance, A-4, A-7
 - reschedule_instance, A-5, A-7
 - resume_instance, A-5
 - save_procedure, A-5, A-7
 - save_procedure_input, A-2
 - stop_instance, A-5
 - submit_procedure, A-5
 - suspend_instance, A-5
 - update_and_retry_step, A-5
 - update_procedure_input, A-2, A-6
- emctl partool utility, C-1
 - emctl partool options, C-2
 - exporting deployment procedure
 - creating PAR file, C-4
 - retrieving GUID, C-3
 - exporting deployment procedures, C-3
 - importing PAR files, C-4
 - using cloud control, C-5
 - using command line, C-5
 - overview, C-1
 - overview of PAR, C-1
 - software library, C-3
- enabling facet synchronization
 - custom configurations, 26-37
- enterprise manager users
 - designers, 2-17
 - operators, 2-17
 - super administrators, 2-17

- error handling modes
 - continue on error, 33-11
 - inherit, 33-11
 - skip target, 33-11
 - stop on error, 33-11
- excluding relationships from custom topology
 - views, 26-74
- exporting
 - comparison template, 26-18
 - custom configuration, 26-38
- extend Oracle RAC, 10-1
 - prerequisites, 10-2

F

- file synchronization, 26-31
- format-specific parsers, 26-48

G

- Galaxy CFG
 - parser, 26-49
 - parser parameters, 26-50
- generic system, and new relationships, 26-68
- GNS settings, 7-19
- gold image
 - provisioning Oracle database replay client using gold image, 12-5
 - provisioning Oracle RAC using gold image, 9-9

H

- hardware configuration, collecting information, 26-2
- history, of configuration changes, 26-11
- history, of configurations, 1-3
- Hosts Access parser, 26-52

I

- ignore rule example, in comparisons, 26-23
- ignore rule, in comparisons, 26-20
- impact analysis, 26-73
- importing
 - comparison template, 26-18
 - custom configuration, 26-38
- including relationships in custom topology
 - views, 26-74
- information map, 1-4
- infrastructure requirements, 2-1
- Introscope parser, 26-49
- inventory and usage details, 26-10

J

- Java Policy parser, 26-54
- Java Properties parser, 26-54
- job activity
 - comparisons, 26-28
 - history, 26-15

K

Kernel Modules parser, 26-52
key properties, 26-31

L

LDAP parser, 26-54
lifecycle management
 overview, 1-1
 solution areas, 1-1
 change management, 1-3
 compliance management, 1-3
 configuration management, 1-3
 discovery, 1-2
 patching, 1-3
 provisioning, 1-2
 solution descriptions, 1-2
Linux Directory List parser, 26-52
linux patching
 prerequisites, 25-3
 setting up group, 25-6
lock down, 32-14
locking down feature, 4-2
logical operators
 AND/OR, 26-24

M

Management Repository, 26-1
mandatory infrastructure requirements
 creating user accounts, 2-16
 setting up credentials, 2-4
mandatory infrastructure requirements
 setting up software library, 2-2
matching rule example, for comparisons, 26-22
matching rule, in comparisons, 26-19
metadata XML files
 creating refresh job, 24-18
 downloading files, 24-17
 uploading files, 24-18
Middleware Provisioning
 Cloning a Middleware Home from an Existing
 Installation, 15-18
 Cloning a WebLogic Domain From an Existing
 Installation, 15-10
 Cloning From a WebLogic Domain Provisioning
 Profile, 15-21
 Cloning from an Oracle Middleware Home Gold
 Image, 15-23
 Creating Software Library Components, 15-6
 Middleware Provisioning and Scale Up / Scale
 Out Best Practices, 16-6
 Scaling Up / Scaling Out WebLogic
 Domains, 16-1
Mime Types parser, 26-54
MQ-Series
 parser, 26-49
 parser parameters, 26-51

N

nondeployable plan, 24-5
notifications, 2-20

O

Odin parser, 26-49
optional infrastructure requirements
 configuring pdp, 2-9
optional infrastructure requirements
 host configurations, E-30
 self update for provisioning, 2-19
 setting up e-mail notifications, 2-20
Oracle Clusterware Clone, 4-17
Oracle Database Clone, 4-15
Oracle Database topology, 5-2
Oracle ORA parser, 26-49
Oracle RAC database topology, 7-2
Oracle Real Application Clusters Database
 topology, 7-2
Oracle Service Bus, 20-1

P

PAM Configuration parser, 26-52
parsers
 AIX Installed Packages, 26-54
 Apache HTTPD, 26-54
 Autosys, 26-54
 Blue Martini DNA, 26-48
 columnar, 26-52
 Connect:Direct, 26-48
 Cron Access, 26-52
 Cron Directory, 26-52
 CSV, 26-52
 Custom CFG, 26-54
 Database Query, 26-48
 Db2, 26-48
 Directory, 26-48
 E-Business Suite, 26-49
 format-specific, 26-48
 Galaxy CFG, 26-49
 Hosts Access, 26-52
 Introscope, 26-49
 Java Policy, 26-54
 Java Properties, 26-54
 Kernel Modules, 26-52
 LDAP, 26-54
 Linux Directory List, 26-52
 Mime Types, 26-54
 MQ-Series, 26-49
 Odin, 26-49
 Oracle ORA, 26-49
 PAM Configuration, 26-52
 Process Local, 26-52
 properties, 26-54
 Radia, 26-54
 Sectioned Properties, 26-55
 Secure TTY, 26-52
 Siebel, 26-49

- SiteMinder Agent, 26-55
- SiteMinder Registry, 26-55
- SiteMinder Report, 26-55
- SmWalker, 26-55
- Solaris Installed Packages, 26-52
- Sun ONE Magnus, 26-55
- Sun ONE Obj, 26-55
- Tuxedo, 26-55
- UbbConfig, 26-49
- Unix Config, 26-55
- Unix Crontab, 26-52
- Unix Directory List, 26-52
- Unix Groups, 26-53
- Unix GShadow, 26-53
- Unix Hosts, 26-53
- Unix INETD, 26-53
- Unix Installed Patches, 26-49
- Unix Login, 26-55
- Unix Passwd, 26-53
- Unix PROFTPD, 26-55
- Unix Protocols, 26-53
- Unix Recursive Directory List, 26-49
- Unix Resolve, 26-55
- Unix Services, 26-53
- Unix Shadow, 26-53
- Unix SSH Config, 26-55
- Unix System, 26-55
- Unix System Crontab, 26-53
- Unix VSFTPD, 26-55
- Unix XINETD, 26-55
- WebAgent, 26-55
- WebLogic (attribute-keyed), 26-46
- WebSphere (attribute-keyed), 26-46
- WebSphere (generic), 26-47
- Windows Checksum, 26-55
- XML (generic), 26-46
- XML default (attribute-keyed), 26-45
- patch management solution
 - accessing the screen, 24-3
 - introduction, 24-2
 - patching modes
 - in-place mode, 24-10
 - offline mode
 - enabling, 24-17
 - overview, 24-10
 - online mode
 - enabling, 24-15
 - overview, 24-10
 - out-of-place mode, 24-11
 - parallel mode, 24-13
 - rolling mode, 24-12
 - patching workflow, 24-13
 - supported targets, 24-8
- patch plans
 - accessing patch plans, 24-31
 - analyzing plans, 24-32
 - creating patch plans, 24-30
 - customizing plans, 24-50
 - deleting plans, 24-48
 - deploying plans, 24-32
 - overview, 24-3
 - patch plan types, 24-5
 - roles and privileges, 24-14
 - saving as patch templates, 24-38
 - supported patch types, 24-3
 - using create plan wizard, 24-5
 - validation and conflict resolution, 24-6
- patch recommendations, 24-26
- patch templates
 - deleting templates, 24-48
 - modifying templates, 24-45
 - overview, 24-7
 - using edit template wizard, 24-7
 - viewing templates, 24-45
- patching
 - analyzing the environment, 24-24
 - diagnosing issues, 24-42
 - identifying applicable patches
 - searching in software library, 24-29
 - searching on MOS, 24-28
 - using knowledge articles, 24-28
 - using patch recommendations, 24-26
 - introduction, 24-1
 - linux patching, 25-1
 - patch management solution, 24-2
 - patching linux hosts, 25-1
 - resolving issues, 24-43
- pdp
 - power broker, 2-9
 - SUDO, 2-9
- pdp templates, 2-12
- phases
 - parallel, 32-10
 - rolling, 32-10
- post-parsing rules, 26-61
- privileges, for custom configurations, 26-39
- Process Local parser, 26-52
- properties parser constructs
 - delimited section, 26-60
 - delimited structure, 26-59
 - element cell, 26-61
 - explicit property, 26-58
 - implicit property, 26-59
 - INI section, 26-60
 - keyword name property, 26-58
 - keyword property, 26-58
 - reserved directive, 26-59
 - reserved function, 26-59
 - simple property, 26-58
 - structure, 26-60
 - XML structure, 26-59
- properties parsers, 26-54
 - advanced constructs, 26-57
 - advanced parameters, 26-56
 - basic parameters, 26-55
- provision database
 - Grid Infrastructure and Oracle RAC Database, 7-3
 - Oracle Grid Infrastructure and Oracle Real

- Application Clusters, 7-1
- provision Linux, 23-1
 - getting started, 23-1
- provision Oracle RAC database
 - with file system on a new cluster, 7-16
 - with file system on an existing cluster, 7-11
- provision Oracle RAC databases, 7-16
- provisioning
 - deleting or scaling down Oracle RAC (Real Application Cluster), 11-1
 - extending Oracle RAC (Real Application Cluster), 10-1
 - provisioning linux operating system, 23-1
 - provisioning Oracle Application Server, 19-1, 22-1
 - provisioning Oracle BPEL processes, 21-1
 - provisioning Oracle database replay client, 12-1
 - provisioning Oracle Service Bus resources, 20-1
- provisioning bare metal servers, 23-16
- provisioning database client
 - getting started, 12-1
- Provisioning Oracle BPEL Processes, 21-2
 - Deployment Procedure, 21-2
 - Getting Started, 21-1
 - Provisioning Procedure, 21-3
- provisioning Oracle Database client, 12-8
- provisioning Oracle Real Application Clusters One database, 8-2
- provisioning profiles, 4-2
- provisioning SOA artifacts, 19-4
 - gold image, 19-6

R

- Radia parser, 26-54
- real-time monitoring facets, 27-61
 - about, 27-61
 - changing base attributes, 27-68
 - creating, 27-64
 - creating like, 27-67
 - deleting, 27-66
 - editing, 27-64
 - entity types, 27-62
 - exporting, 27-67
 - importing, 27-67
 - operations on, 27-63
 - patterns, 27-62
 - viewing library, 27-63
- real-time monitoring rule
 - compliance score, 27-17
- real-time monitoring rules
 - compliance standard rules, 27-45
- reference host, 23-3
- relationships, 26-68
- repository rules
 - in compliance standards, 27-44
- resubmit comparison job, 26-28
- reverse transform, 26-32
- roles
 - EM_ALL_DESIGNER, 2-17

- EM_ALL_OPERATOR, 2-18
- roles, for custom configurations, 26-39
- rollup options, 26-11
- root cause analysis. See dependency analysis
- RPM repository, 23-3
 - overview, 23-3
 - setting up, 23-7, 25-4
- rule examples, for comparisons, 26-22
- rule expressions, in comparisons, 26-20
- rules, in comparisons, 1-3, 26-19
- rules, in custom configurations, 26-36

S

- save as draft, custom configuration, 26-38
- saved configurations, 26-9
- scale down Oracle RAC, 11-5
- Scaling Up / Scaling Out WebLogic Domains
 - Prerequisites, 16-3
 - Running the Scale Up / Scale Out Middleware Deployment Procedure, 16-4
- schedule comparison, 26-27
- schema baseline, 28-2
 - multiple versions, 28-6
- schema baseline version, 28-4
- schema baselines
 - export, 28-8
 - import, 28-8
 - overview, 28-2
- schema change plans, 28-2
- schema comparison, 28-2
- schema comparisons
 - overview, 28-9
- schema synchronization, 28-2
 - overview, 28-13
 - versions, 28-17
- scope specification, 28-3
- search configurations
 - predefined, 1-3, 26-3
 - user-defined, 1-3, 26-3
- Sectioned Properties parser, 26-55
- Secure TTY parser, 26-52
- security metrics
 - enabling, 27-42
- setting up
 - named credentials, 2-6
 - privileged credentials, 2-8
- Setting Up MOS, 2-19
- Siebel
 - parser, 26-49
 - parser parameters, 26-51
- SiteMinder Agent parser, 26-55
- SiteMinder Registry parser, 26-55
- SiteMinder Report parser, 26-55
- SmWalker parser, 26-55
- software library
 - uploading patch, 24-20
- Software Library Administration, 2-3, 2-4
- Software Library console, 2-3
- Solaris Installed Packages parser, 26-52

- specify OS users, 7-17
- SQL, using in a configuration search, 26-5
- stage server, 23-3
 - overview, 23-3
 - setting up, 23-4
- steps
 - action, 32-11
 - computational, 32-10
 - file transfer, 32-11
 - host command, 32-12
 - job, 32-11
 - library component, 32-12
 - library directive, 32-12
 - manual, 32-10
- Sun ONE Magnus parser, 26-55
- Sun ONE Obj parser, 26-55
- synchronizing files, 26-31
- system comparison results, 26-29
- system component structure, 26-71

T

- target type, custom, 26-33
- template, selecting for comparison, 26-26
- testing pdp settings, 2-13
- topology
 - Oracle RAC database topology, 7-2
- topology viewer
 - controlling appearance of information on a graph, 26-76
 - creating
 - relationships to a target, 26-75
 - customizing views, 26-73
 - deleting custom views, 26-74
 - deleting relationships from a target, 26-75
 - dependency analysis, 26-73
 - excluding relationships from custom views, 26-74
 - impact analysis, 26-73
 - including relationships in custom views, 26-74
- tracking configuration changes, 26-11
- Tuxedo parser, 26-55

U

- UbbConfig parser, 26-49
- undeploying custom configuration, 26-40
- Unix Config parser, 26-55
- Unix Crontab parser, 26-52
- Unix Directory List parser, 26-52
- Unix Groups parser, 26-53
- Unix GShadow parser, 26-53
- Unix Hosts parser, 26-53
- Unix INETD parser, 26-53
- Unix Installed Patches
 - parser, 26-49
 - parser parameters, 26-51
- Unix Login parser, 26-55
- Unix Passwd parser, 26-53
- Unix PROFTPD parser, 26-55
- Unix Protocols parser, 26-53

- Unix Recursive Directory List
 - parser, 26-49
 - parser parameters, 26-51
- Unix Resolve parser, 26-55
- Unix Services parser, 26-53
- Unix Shadow parser, 26-53
- Unix SSH Config parser, 26-55
- Unix System Crontab parser, 26-53
- Unix System parser, 26-55
- Unix VSFTPD parser, 26-55
- Unix XINETD parser, 26-55
- updating pdp settings
 - EM console, 2-12
 - sudoers file, 2-10
- upgrading a database instance, 14-8
- upgrading database, 14-4
 - getting started, 14-1
- uploading patches
 - identifying patch details, 24-21
 - uploading to software library, 24-22
- user accounts
 - overview, 2-16
- User Defined Deployment Procedure, 32-13
- UTF-8, encoding in custom configurations, 26-34

V

- value constraint rule, in comparisons, 26-19
- viewing
 - comparison template, 26-18
 - configuration data, 26-8
 - configuration health problem details, 26-72
 - custom configuration specification details, 26-37

W

- WebAgent parser, 26-55
- WebLogic parser (attribute-keyed), 26-46
- WebLogic Server Signature Rules
 - in compliance standards, 27-44
- WebSphere parser (attribute-keyed), 26-46
- WebSphere parser (generic), 26-47
- Windows Checksum parser, 26-55

X

- XML default parser (attribute-keyed), 26-45
- XML parser (generic), 26-46
- XPath
 - conditions and expressions, 26-61
 - custom configuration, 26-36

