

Oracle® Enterprise Manager

Administrator's Guide



24ai Release 1 (24.1)

F97191-06

August 2025

ORACLE®

Copyright © 2016, 2025, Oracle and/or its affiliates.

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, software documentation, data (as defined in the Federal Acquisition Regulation), or related documentation that is delivered to the U.S. Government or anyone licensing it on behalf of the U.S. Government, then the following notice is applicable:

U.S. GOVERNMENT END USERS: Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs) and Oracle computer documentation or other Oracle data delivered to or accessed by U.S. Government end users are "commercial computer software," "commercial computer software documentation," or "limited rights data" pursuant to the applicable Federal Acquisition Regulation and agency-specific supplemental regulations. As such, the use, reproduction, duplication, release, display, disclosure, modification, preparation of derivative works, and/or adaptation of i) Oracle programs (including any operating system, integrated software, any programs embedded, installed, or activated on delivered hardware, and modifications of such programs), ii) Oracle computer documentation and/or iii) other Oracle data, is subject to the rights and limitations specified in the license contained in the applicable contract. The terms governing the U.S. Government's use of Oracle cloud services are defined by the applicable contract for such services. 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®, Java, MySQL, and NetSuite are registered trademarks of Oracle and/or its affiliates. Other names may be trademarks of their respective owners.

Intel and Intel Inside 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, Epyc, and the AMD 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 about 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 unless otherwise set forth in an applicable agreement between you and Oracle. 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, except as set forth in an applicable agreement between you and Oracle.

Contents

Preface

Audience	i
Documentation Accessibility	i
Related Documents	i
Conventions	i

Part I Administering Oracle Enterprise Manager

1 Maintaining Enterprise Manager

Overview: Manage Enterprise Manager	1
Health Overview	2
Viewing Enterprise Manager Topology and Charts	3
Determining Enterprise Manager Page Performance	3
Repository	8
Repository Tab	8
Metrics Tab	13
Schema Tab	15
Controlling and Configuring Management Agents	16
Manage Agents Page	16
Agent Home Page	16
Controlling a Single Agent	17
Configuring Single Management Agents	17
Controlling Multiple Management Agents	18
Configuring Multiple Agents	18
Upgrading Multiple Management Agents	19
Management Servers	19
Job System Diagnostics	20
Compliance Standards	20

2 Maintaining and Troubleshooting the Management Repository

Management Repository Deployment Guidelines	1
---	---

Management Repository Data Retention Policies	2
Management Repository Default Aggregation and Purging Policies	2
Management Repository Default Aggregation and Purging Policies for Other Management Data	4
Modifying the Default Aggregation and Purging Policies	5
How to Modify the Retention Period of Job History	6
DBMS_SCHEDULER Troubleshooting	7
Dropping and Recreating the Management Repository	9
Dropping the Management Repository	9
Recreating the Management Repository	10
Using a Connect Descriptor to Identify the Management Repository Database	10
Troubleshooting Management Repository Creation Errors	11
Package Body Does Not Exist Error While Creating the Management Repository	11
Server Connection Hung Error While Creating the Management Repository	11
General Troubleshooting Techniques for Creating the Management Repository	12
Cross Platform Enterprise Manager Repository Database Migration	13
Introduction to RepMigrate	14
How to Get RepMigrate Utility?	14
RepMigrate Usage	14
Repository Migration Steps Using RepMigrate	15
Step 1. Prepare Databases	15
Step 2. Best Practices	18
Step 3. Run Prerequisites Check	20
Step 4. Perform Migration	21
Perform Post Migration Verification	28
RepMigrate Files and Troubleshooting	28
RepMigrate Log Files	28
RepMigrate Response Files	29
Troubleshoot RepMigrate	31

3 Configuring a Software Library

Overview of Software Library	1
Users, Roles, and Privileges	2
Performing Software Library Tasks Using EM CLI Verbs or in Graphical Mode	4
Software Library Storage	7
Upload File Locations	9
Referenced File Location	10
Cache Nodes	11
Prerequisites for Configuring Software Library	11
Configuring Software Library Storage Location	12
Configuring an OMS Shared File system Location	12

Configuring an OMS Agent File system Location	13
Configuring a Referenced File Location	15
Configuring Software Library on a Multi-OMS System	16
Software Library Cache Nodes	16
Configuring the Cache Nodes	16
Adding Cache Nodes	17
Editing the Cache Nodes	18
Deleting the Cache Nodes	19
Activating or Deactivating the Cache Nodes	19
Clearing the Cache Nodes	19
Synchronizing the Cache Nodes	19
Exporting and Importing Files for Cache Nodes	20
Export	20
Import	20
Software Library File Transfers	20
Using Software Library Entities	21
Tasks Performed Using the Software Library Home Page	22
Organizing Entities	22
Creating Entities	23
Creating Generic Components	23
Creating Directives	25
Customizing Entities	27
Managing Entities	27
Accessing Software Library Home Page	28
Accessing Software Library Administration Page	28
Granting or Revoking Privileges	28
Moving Entities	29
Changing Entity Maturity	29
Adding Notes to Entities	29
Adding Attachments to Entities	30
Viewing, Editing, and Deleting Entities	30
Purging Deleted Entities	31
Searching Entities	31
Exporting Entities	33
Importing Entities	33
Staging Entities	34
Maintaining Software Library	35
Periodic Maintenance Tasks	35
Re-Importing Oracle Owned Entity Files	36
Removing (and Migrating) Software Library Storage Location	36
Removing a Referenced Storage Location	38
Deactivating and Activating a Storage Location	38

Scheduling Purge Job	39
Backing Up Software Library	39

4 Managing Plug-Ins

Getting Started	1
Introduction to Plug-ins	2
Enterprise Manager Extensibility Paradigm	2
Plug-Ins	3
Plug-Ins Deployed by Default	3
Plug-In Releases	3
Obsolete and Deprecated Plug-ins	4
Roles Required to Manage Plug-Ins	4
Workflow of Plug-In Deployment	4
Introduction to Plug-In Manager	8
Accessing Plug-In Manager	8
Performing Operations Using Plug-In Manager	8
Knowing Your Plug-Ins	9
Customizing Your View	9
Customizing Displayed Plug-Ins	9
Customizing Displayed Columns	10
Checking the Availability of Plug-Ins	10
Viewing Information about Plug-Ins	10
Differentiating Plug-In Releases from Enterprise Manager Platform Releases	11
Identifying Plug-In ID	12
Viewing Targets and Operating Systems Certified for Deployed Plug-Ins	12
Viewing Plug-In Dependencies	12
Verifying Deployed Plug-Ins	13
Downloading, Deploying, and Upgrading Plug-Ins	14
Downloading Plug-Ins	14
Downloading Plug-Ins in Online Mode	14
Downloading Plug-Ins in Offline Mode	15
Importing Catalog Archives	15
Importing Plug-In Archives	16
Deploying Plug-Ins to Oracle Management Service (Reduce OMS Restart time and Downtime)	17
Tracking the Deployment Status of Plug-Ins on Oracle Management Service	21
Upgrading Plug-Ins Deployed to Oracle Management Service	21
Deploying Plug-Ins on Oracle Management Agent	21
Tracking the Deployment Status of Plug-Ins on Oracle Management Agent	22
Upgrading Plug-Ins Deployed to Oracle Management Agent	22
Undeploying Plug-Ins	23

Undeploying Plug-Ins from Oracle Management Service	23
Undeploying Plug-Ins from Oracle Management Agent	25
Advanced Operations with Plug-Ins	26
Re-deploying Plug-Ins on Oracle Management Agent	26
Deploying Plug-In Patches While Deploying or Upgrading Management Agent (Create Custom Plug-In Update)	27
Creating Custom Plug-In Update Using EMCLI	28
Creating Custom Plug-In Update Using EDK	29
Troubleshooting	30
Understanding Plug-In Homes	30
Troubleshooting OMS Plug-In Deployment and Upgrade Issues	31
Troubleshooting OMS Plug-In Deployment Issues	31
Rollback and Resume OMS Plug-In Upgrade	31
Troubleshooting Management Agent Plug-In Deployment, Upgrade, and Blocked Issues	32
Troubleshooting Management Agent Plug-In Deployment Issues	32
Troubleshooting Management Agent Plug-In Upgrade Issues	32
Resolving a Plug-in Mismatch on a Management Agent	33
Running a Plug-in Mismatch Job to Resolve All Plug-in Mismatches	33

5 Patching and Updating Enterprise Manager

Updating Enterprise Manager	1
Using Self Update	1
What Can Be Updated?	1
Setting Up Self Update	2
Setting Up Enterprise Manager Self Update Mode	2
Assigning Self Update Privileges to Users	3
Setting Up the Software Library	3
Setting My Oracle Support Preferred Credentials	3
Registering the Proxy Details for My Oracle Support	4
Setting Up the EM CLI Utility (Optional)	4
Applying an Update	5
Applying an Update in Online Mode	5
Applying an Update in Offline Mode	6
Accessing Informational Updates	6
Acquiring or Updating Management Agent Software	7
Patching Oracle Management Service and the Repository	7
OMSPatcher Automation	8
Supported OMS Configurations and OMSPatcher Patchability	8
Oracle Universal Installer Inventory Configurations (OUI)	9
Supported Patch Format	10
Supported Patching Methodologies	11

Required OMSPatcher Parameters	11
Creating a Property File	11
Prerequisites for Running OMSPatcher	14
Using OMSPatcher	14
My Oracle Support: Searching for Patches	15
Checking System Prerequisites	16
Running omspatcher apply	17
Running omspatcher rollback	24
Running omspatcher lspatches	26
Running omspatcher version	26
Running Zero Downtime Commands	26
Patching a Standby OMS System	27
Patching with Non-SYS User (Admin User)	27
OMSPatcher Command Syntax	30
Apply	31
Rollback	33
lspatches	35
version	36
checkApplicable	36
saveConfigurationSnapshot	37
Zero Downtime Patching	38
OMSPatcher Command Updates	40
Zero Downtime Patching Workflow	41
Patching Use Cases	43
Applying MRS Artifacts	45
Post-Patching Verification	46
Holistic Patching	46
Troubleshooting	48
OMSPatcher Troubleshooting	48
OMSPatcher Log Management	49
Logs for Oracle Support	51
OMSPatcher: Cases Analysis, Error Codes, and Remedies/Suggestions	52
OMSPatcher: External Utilities Error Codes	53
Special Error Cases for OMSPatcher OMS Automation	54
OMSPatcher Session Resume	57
Resume capability in Single-OMS Configuration	57
Resume Capability in Multi-OMS Configuration	60
Patching Oracle Management Agents	63
Overview	63
Automated Management Agent Patching Using Patch Plans (Recommended)	64
Advantages of Automated Management Agent Patching	65
Accessing the Patches and Updates Page	65

Viewing Patch Recommendations	65
Searching for Patches	66
Applying Management Agent Patches	67
Verifying the Applied Management Agent Patches	71
Management Agent Patching Errors	72
Manual Management Agent Patching	73

6 Personalizing Enterprise Manager

Personalizing a Enterprise Manager Page	1
Customizing a Region	2
Setting Your Homepage	2
Setting Pop-Up Message Preferences	3

7 Administering Enterprise Manager Using EMCTL Commands

Executing EMCTL Commands	1
Guidelines for Starting Multiple Enterprise Manager Components on a Single Host	2
Starting and Stopping Oracle Enterprise Manager	2
Starting Enterprise Manager and All Its Components	2
Stopping Enterprise Manager and All Its Components	3
Services That Are Started with Oracle Management Service Startup	4
Starting and Stopping the Oracle Management Service and Management Agent on Windows	4
Reevaluating Metric Collections Using EMCTL Commands	5
Specifying New Target Monitoring Credentials in Enterprise Manager	6
EMCTL Commands for OMS	7
EMCTL Commands for Management Agent	12
EMCTL Security Commands	16
EMCTL Secure Commands	16
Security diagnostic commands	19
EMCTL EM Key Commands	20
Configuring Authentication	21
Configuring OSSO Authentication	22
Configuring OAM Authentication	23
Configuring LDAP (OID and AD) Authentication	23
Configuring Repository Authentication (Default Authentication)	23
EMCTL HAConfig Commands	24
EMCTL Resync Commands	25
EMCTL Connector Command	25
EMCTL Patch Repository Commands	26
EMCTL Commands for Windows NT	26
EMCTL Partool Commands	27

EMCTL Plug-in Commands	28
EMCTL Command to Sync with OPSS Policy Store	28
Troubleshooting Oracle Management Service Startup Errors	28
Troubleshooting Management Agent Startup Errors	29
Management Agent starts up but is not ready	29
Management Agent fails to start due to time zone mismatch between agent and OMS	30
Management Agent fails to start due to possible port conflict	30
Management Agent fails to start due to failure of securing or unsecuring	30
Using emctl.log File to Troubleshoot	30

8 Locating and Configuring Enterprise Manager Log Files

Managing Log Files	1
Viewing Log Files and Their Messages	3
Restricting Access to the View Log Messages Menu Item and Functionality	4
Registering Additional Log Files	4
Searching Log Files	5
Searching Log Files: Basic Searches	6
Searching Log Files: Advanced Searches	7
Downloading Log Files	7
Managing Saved Searches	9
Saving Searches	9
Retrieving Saved Searches	9
Managing Saved Searches	9
Locating Management Agent Log and Trace Files	10
About the Management Agent Log and Trace Files	10
Structure of Agent Log Files	11
Locating the Management Agent Log and Trace Files	11
Setting Oracle Management Agent Log Levels	12
Modifying the Default Logging Level	13
Setting gcagent.log	13
Setting gcagent_error.log	13
Setting the Log Level for Individual Classes and Packages	13
Setting gcagent_mdu.log	14
Setting the TRACE Level	16
Locating and Configuring Oracle Management Service Log and Trace Files	16
About the Oracle Management Service Log and Trace Files	16
Locating Oracle Management Service Log and Trace Files	17
Controlling the Size and Number of Oracle Management Service Log and Trace Files	17
Controlling the Contents of the Oracle Management Service Trace File	18
Controlling the Oracle WebLogic Server and Oracle HTTP Server Log Files	19
Monitoring Log Files	21

About Log Viewer	21
Overview of WebLogic Server and Application Deployment Log File Monitoring	22
Enabling Log File Monitoring	22
Configuring Log File Monitoring	23
Viewing Alerts from Log File Monitoring	25
Configuring Log Archive Locations	25

9 Configuring and Using Services

Introduction to Services	1
Defining Services in Enterprise Manager	1
Creating a Service	2
Creating a Generic Service - Test Based	2
Creating a Generic Service - System Based	3
Creating an Aggregate Service	3
Monitoring a Service	4
Viewing the Generic / Aggregate Service Home Page	4
Viewing the Performance / Incidents Page	5
Viewing the SLA Dashboard	5
Viewing the Test Summary	5
Viewing the Service Topology	6
Sub Services	6
Configuring a Service	6
Availability Definition (Generic and Aggregate Service)	7
Root Cause Analysis Configuration	8
Getting the Most From Root Cause Analysis	8
System Association	9
Monitoring Settings	9
Service Tests and Beacons	10
Defining Additional Service Tests	10
Deploying and Using Beacons	11
Configuring the Beacons	12
Performance Metrics	13
Rule Based Target List	15
Static Based Target List	15
Usage Metrics	15
Setting Up and Using Service Level Agreements	16
Actionable Item Rules for SLAs	18
Creating a Service Level Objective	19
Lifecycle of an SLA	20
Viewing the Status of SLAs for a Service	21
Defining Custom SLA Business Calendars	22

Using the Services Dashboard	22
Viewing the All Dashboards Page	22
Viewing the Dashboard Details Page	23
Customizing and Personalizing the Dashboard	23
Viewing the Dashboard Service Details Page	24
Using the Test Repository	25
Viewing the Test Repository	25
Editing an ATS Script	26
Configuring Service Levels	26
Defining Service Level Rules	27
Viewing Service Level Details	28
Configuring a Service Using the Command Line Interface	28

10 Connecting to Enterprise Manager Desktop Version

Part II Integrating with Oracle Cloud Infrastructure

11 Integrating Enterprise Manager with OCI Services

Prerequisites	2
Setting Up OCI Service Connectivity	5
Step 1: Export Enterprise Manager Data to OCI	5
Step 2: Import Data from the Object Storage Bucket to the OCI Service	7
Viewing Data Upload Status for a Service	8
Monitoring Data Uploads from Enterprise Manager	10
Adding Target Groups to OCI Services	14
Managing Cloud Bridges	14
Viewing Cloud Extension Data	14
Configuring Cloud Extension	15

12 Generative AI Assistant

About Ask EM	1
Configuring Ask EM	2

Part III Generating Reports

13	Controlling Resource Usage	
	Repository Session (SQL) Throttling	1
	Application API Throttling	3
14	Creating Dashboards Using Grafana	
15	Using Information Publisher	
	About Information Publisher	1
	Out-of-Box Report Definitions	2
	Custom Reports	2
	Creating Custom Reports	2
	Report Parameters	3
	Report Elements	3
	Scheduling Reports	3
	Flexible Schedules	3
	Storing and Purging Report Copies	4
	E-mailing Reports	4
	Sharing Reports	4
16	Standalone Oracle Analytics Server	
	Index	

Preface

This guide describes how to use Oracle Enterprise Manager core functionality.

Audience

This document is intended for Enterprise Manager administrators and developers who want to manage their Enterprise Manager infrastructure.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For the latest releases of Enterprise Manager and other Oracle documentation, see:

<http://docs.oracle.com/en/enterprise-manager/>

Conventions

The following text conventions are used in this document:

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

Part I

Administering Oracle Enterprise Manager

This section contains the following chapters:

- [Maintaining Enterprise Manager](#)
- [Maintaining and Troubleshooting the Management Repository](#)
- [Updating Enterprise Manager](#)
- [Configuring a Software Library](#)
- [Managing Plug-Ins](#)
- [Patching Oracle Management Service and the Repository](#)
- [Patching Oracle Management Agents](#)
- [Personalizing Enterprise Manager](#)
- [Administering Enterprise Manager Using EMCTL Commands](#)
- [Locating and Configuring Enterprise Manager Log Files](#)
- [Configuring and Using Services](#)
- [Connecting to Enterprise Manager Desktop Version](#)

1

Maintaining Enterprise Manager

Enterprise Manager provides extensive monitoring and management capabilities for various Oracle and non-Oracle products. Used to manage your heterogeneous IT infrastructure, Enterprise Manager plays an integral role in monitoring and maintaining the health of your IT resources. It is therefore essential to ensure Enterprise Manager itself is operating at peak efficiency.

To help you maintain your Enterprise Manager installation, a variety of enhanced self-monitoring and diagnostic functionality is available from the Enterprise Manager console. These functions are designed to help you understand and monitor various components of Enterprise Manager, monitor/measure the quality of services Enterprise Manager provides, diagnose failures quickly, and manage Agents more easily.

This chapter covers the following topics:

- [Overview: Manage Enterprise Manager](#)
- [Health Overview](#)
- [Repository](#)
- [Controlling and Configuring Management Agents](#)
- [Management Servers](#)
- [Job System Diagnostics](#)
- [Compliance Standards](#)

Overview: Manage Enterprise Manager

Although Enterprise Manager functions as a single entity to manage your IT infrastructure, in reality it is composed of multiple components working in concert to provide a complete management framework from a functional standpoint. All major components of Enterprise Manager have been grouped into a single system. A special set of services has been created (based on the system) to model Enterprise Manager functions.

Management Features

- Topology view that allows you to see all major components of Enterprise Manager and their current status.
- Dashboard displaying the overall health of Enterprise Manager.
- Full control of the Agent directly from the Enterprise Manager console. Functions include:
 - View/edit Agent configuration properties.
 - View Agent(s) configuration history and compare the results against other Agents.
 - Perform Agent control operations (start/stop/secure).
 - Upgrade Management Agents

Health Overview

The Health Overview provides a comprehensive overview of OMS and Repository operation and performance, and therefore allows you to view the overall health of your Enterprise Manager environment.

Accessing the Health Overview

From the **Setup** menu, select **Manage Enterprise Manager** and then **Health Overview**.

All major areas of Enterprise Manager are represented.

- **Overview:** Provides key information for active Management Services such as the Management Agents, the WebLogic Administration Server, total number of monitored targets, number of administrators, and server load balancer (SLB) upload and console URLs, provided SLB is configured. If configured, the SLB upload and console URLs are also displayed.
- **Repository Details:** Provides physical information about the Management Repository and the host on which the database is located. You can drill down into the database home page for more information and carry out administrative operations.
- **Job System Status:** Displays key operational parameters of the Enterprise Manager Job service. For detailed information, you can click on the status icon to drill down into the Enterprise Manager Job Service home page.
- **Console Activity:** Displays the overall load on the Enterprise Manager console through the average number of requests per minute and the average time required to process those requests.
- **Alerts:** Provides details on the metric errors recorded and when an alert was triggered. In-context links to Incident Manager are also provided.
- **Performance Charts:** Upload Backlog and Upload Rate, Backoff Requests, Notification backlog. You can drill down into any chart to view detailed metric information.
- **Dynamic Runbooks:** Allows you to capture procedural knowledge and expertise in diagnosing and resolving incidents from your subject matter experts and store them in Enterprise Manager for ready access and execution by other Enterprise Manager users. They typically consist of a set of ordered instructions (steps) to resolve the issue.

Starting with Enterprise Manager 13c Release 5 Update 15, **Oracle-provided Runbooks** are available. They are predefined runbooks of various types that help you diagnose and resolve different incidents. For example, you can use the Runbook named: **Loader issues causing Agent backoff requests (Oracle)** to diagnose the agents back off issues. You see an incident message in EM Health that looks like the following: *Health Check: Loader is in FAILURE*. The Runbook steps you through the entire, end to end, analysis and solution. In some cases, some of the steps guide you also visually by showing a video of the data analysis. For more information, see Oracle Provided Runbooks.

From this page, you can carry out all monitoring and management operations using the **OMS and Repository** menu.

Note

The Diagnostic Metrics page is intended for use by Oracle Support when diagnosing issues with the OMS. The page can be accessed by selecting **Monitoring** and then **Diagnostic Metrics** from the **OMS and Repository** menu.

Viewing Enterprise Manager Topology and Charts

The Enterprise Manager Topology page provides a graphical representation of the Enterprise Manager infrastructure components and their association. Each node in the hierarchy displays key information about the member type, the host on which it resides, and the number of incidents, if any. The incident icons on each of the nodes expand to display a global view of current status for each node in the hierarchy.

Note

In order for the Enterprise Manager repository database to appear in the Topology page, you must first manually discover the database. Manual discovery is also required in order to have the database's metric data (Database Time (centiseconds per second)) displayed in the charts.

Accessing Enterprise Manager Topology

1. From the Setup menu, select **Manage Enterprise Manager** and then **Health Overview**.
2. Click the **OMS and Repository** menu to display available operations that can be performed from this page.
3. Select **Members** and then **Topology**.

Enterprise Manager Charts

The Enterprise Manager Charts page displays eight charts representing key areas that together indicate the overall health of Enterprise Manager. These are Overall Files Pending Load -Agent, Job Step Backlog, Job Step Throughput (per second), Request Processing Time (ms), Database Time (centiseconds per second), CPU Utilization (%), Pages Paged-in (per second), Pages Paged-out (per second). Data can be viewed for the Last 24 hours, last 7 days or last 31 days.

Accessing Enterprise Manager Charts

1. From the Setup menu, select **Manage Enterprise Manager** and then **Health Overview**.
2. Click the **OMS and Repository** menu to display available operations that can be performed from this page.
3. Select **Monitoring** and then **Charts**.

Determining Enterprise Manager Page Performance

Page Performance Monitoring and diagnosis feature provides you with the ability to identify and diagnose performance issues with Enterprise Manager pages without having to contact Oracle support.

To access Page Performance Monitoring and Diagnosis functionality:

1. From the **Setup** menu, select **Manage Enterprise Manager**, and then **Health Overview** or **Repository**.
2. From the **OMS and Repository** menu, select **Monitoring** and then **Page Performance**. The Page Performance page displays.

Overview

The overview tab provides details of the overall page performance in Enterprise Manager.



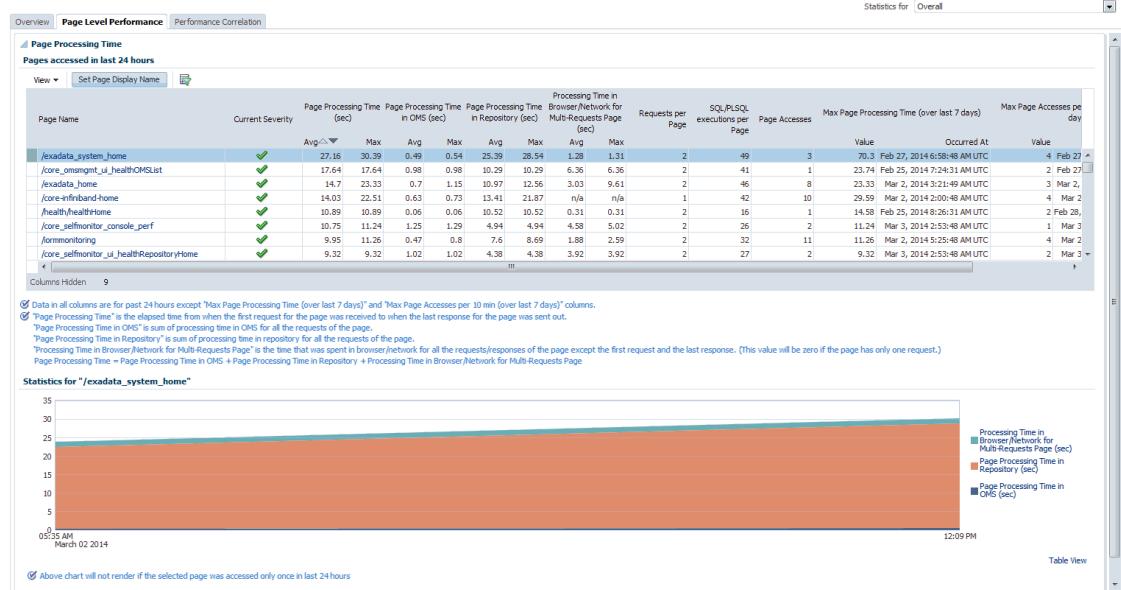
The charts display the Page Accesses and Sessions, Current Page Accesses and Sessions Distribution across OMSs and the Overall Statistics of page performance in the last 24 hours. There are details of the page performance in each of the OMSs as well as the details of the available repositories.

The Overall Statistics table provides the breakdown of times spent in the Repository, the OMS and network and the number of page accesses, the maximum time taken by page in the last 24 hours.

Page Level Performance

The page level performance tab shows the list of pages accessed in the last 24 hours.

Page Performance

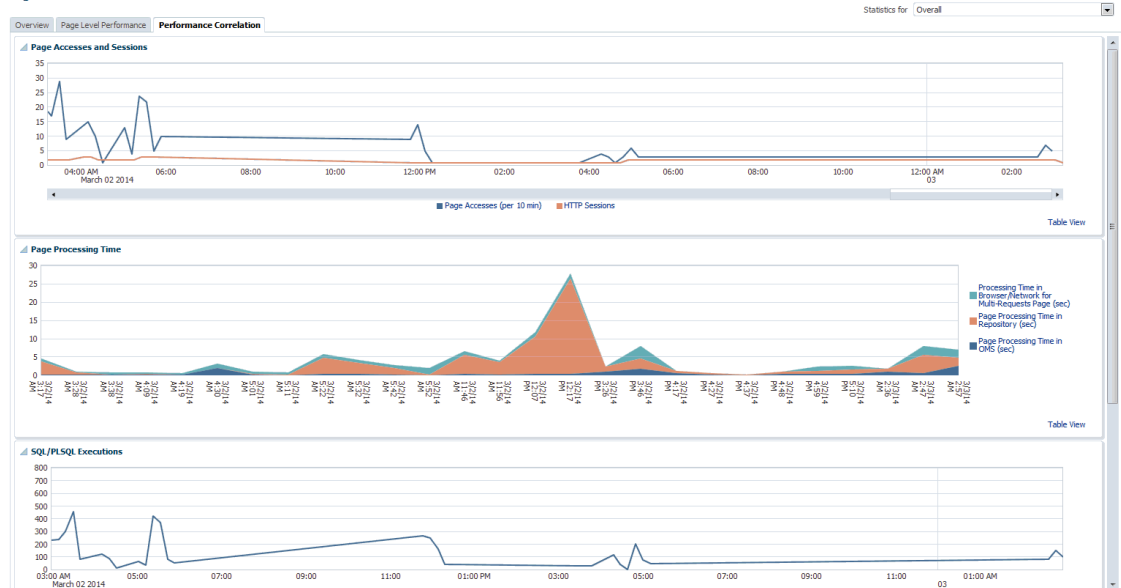


The page also displays the breakdown of time spent in the Repository and the OMS and network in a line graph format for each page.

Performance Correlation

The performance correlation tab displays graphs for page performance that allow you to correlate performance trends.

Page Performance



This tab provides details of page accesses and sessions, page processing time, SQL/PLSQL executions, and average active sessions.

Symptom Diagnosis

Symptom diagnosis can be performed for both overall page processing time and individual page times. Symptom diagnosis is triggered when the set metric thresholds for overall page processing time are exceeded. Diagnosis is accessed by means of an icon in the Overview tab in the Overall Statistics section when the overall page performance threshold is exceeded, as shown in the following graphic.

Figure 1-1 Symptom Diagnosis Icon



For individual pages, the symptom diagnosis icon is displayed in the table in the Current Severity column if the page performance metric threshold is exceeded.

When the icon is displayed in the Overall Statistics section, it indicates that the overall performance of the Enterprise Manager pages has exceeded the threshold in the last 10 minutes. Clicking on the icon, you are taken to another tab where the details of the diagnosis are presented. The diagnosis indicates the root cause for the overall page performance exceeding the metric threshold, the findings that were deduced on diagnosis and the checks that were performed to analyze the overall page performance issue.

The checks are performed at the database level, middle-tier level and the browser/network level to isolate which part of the system might be the cause of the issue. Each check is analyzed and the checks that are identified as the top causes are reported as findings. The topmost finding is then reported as the root cause for the performance issue.

Target Availability Symptom Diagnosis:

Symptom diagnosis can be performed on the availability of the Agent as well. The icon is displayed in the Agent List and Agent Home pages in the event that the Agent target is unreachable or in pending status.

Figure 1-2 Agent List Page

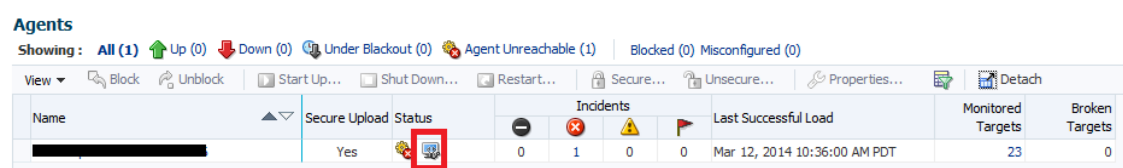
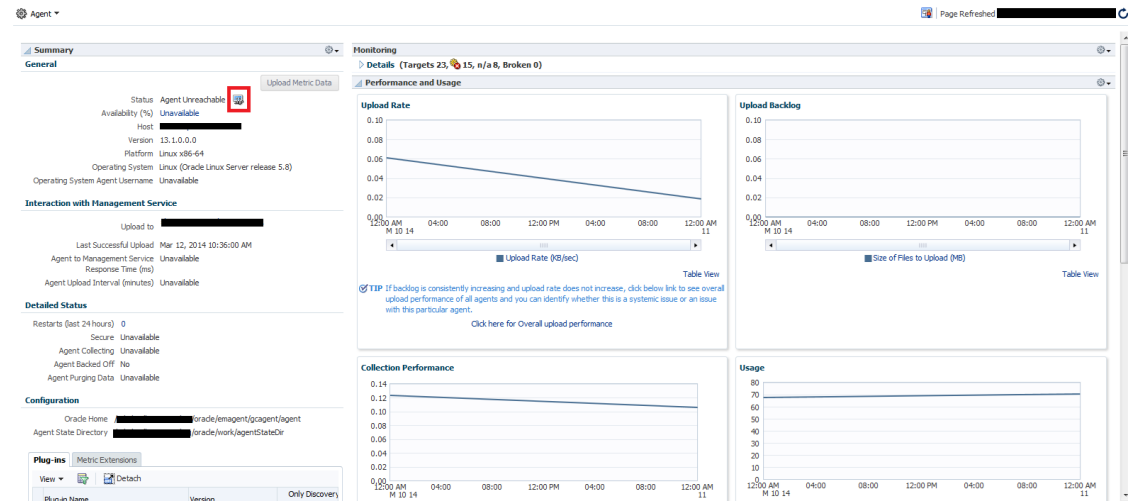


Figure 1-3 Agent Home Page



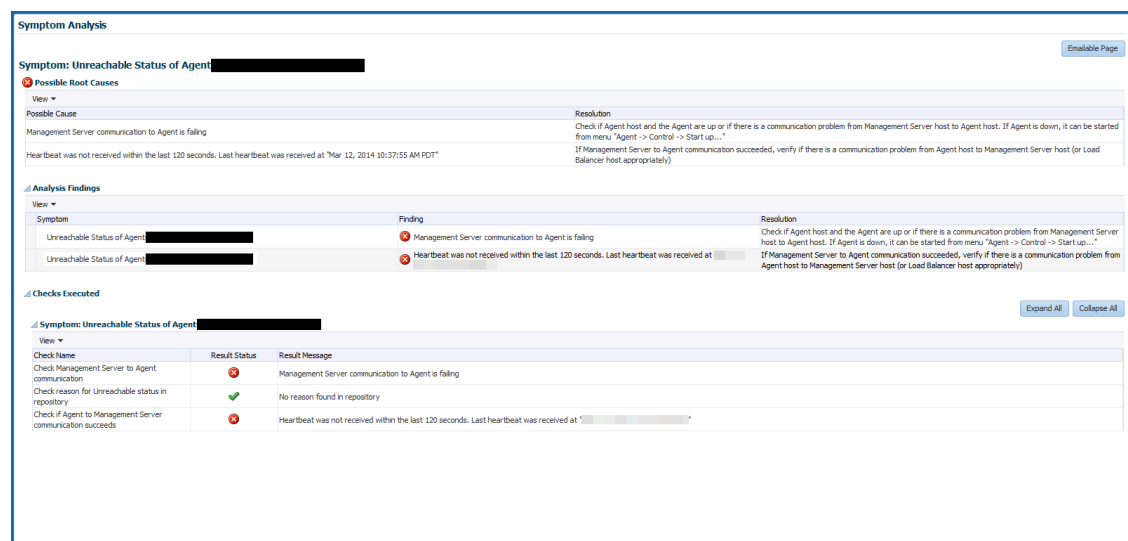
On clicking the icon, the user is navigated to another tab where the details of the diagnosis are presented. The diagnosis indicates the root cause for the Agent's unreachable/pending state, the findings that were deduced from the diagnosis and the checks that were performed to analyze the Agent availability issue.

The checks performed to diagnose the issue consist of the following:

- if the communication between the Management Service and the Agent is successful
- if the Agent has communicated with the Management Service
- if reasons can be deduced from the Repository
- if further reasons can be deduced by performing checks from the Agent side (whether communication between the OMS and the Agent exists).

Each check is analyzed and the checks that are identified as the top causes are reported as findings. The topmost finding is then reported as the root cause for the performance issue.

Figure 1-4 Agent Symptom Diagnosis



Note

If communication between the OMS and Agent cannot be established, then the diagnosis will report findings based on the data available in Management Repository, which may not be the real cause for the issue.

The symptom diagnosis feature is also available in the All Targets page for targets in unreachable or pending status by clicking on the status icon.

Repository

The Repository page provides you with an overview of the status and performance of the Repository DBMS Jobs that handle part of Enterprise Manager's maintenance and monitoring functionality. These DBMS jobs run within the Management Repository and require no user input. Charts showing the key Repository Details and Backlog in Repository Collection are provided. The Scheduler Status region provides the status of the scheduler and the number of Job Queue Processes.

Accessing Repository Information

From the **Setup** menu, select **Manage Enterprise Manager** and then **Repository**.

Three tabs are displayed providing a comprehensive view of repository attributes, performance, as well as access to requisite operational parameters.

- [Repository Tab](#)
- [Metrics Tab](#)
- [Schema Tab](#)

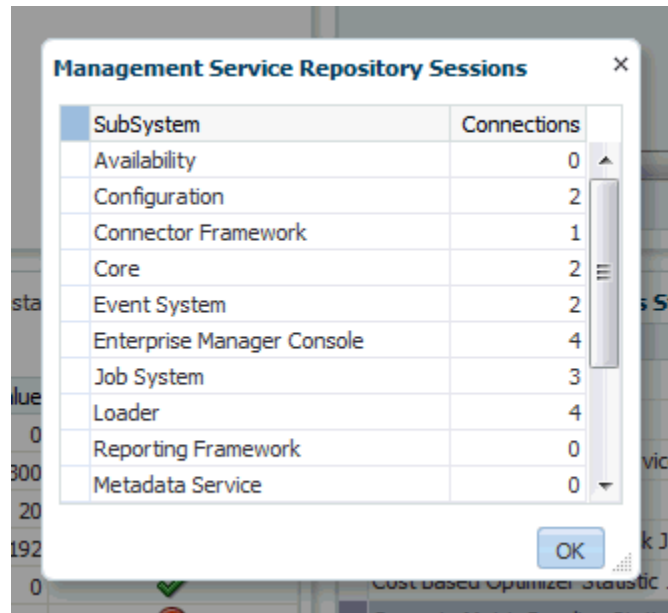
Repository Tab

The Repository tab provides a comprehensive snapshot of repository-specific monitoring.

Repository Details

The Repository Details region provides high-level database information for the Enterprise Manager repository. From this region, you can click on the number **Management Service Repository Sessions** details to view the exact number of repository connections per individual Enterprise Manager subcomponent such as the event system, console, job system, or connector framework.

Figure 1-5 Repository Sessions Per Subcomponent

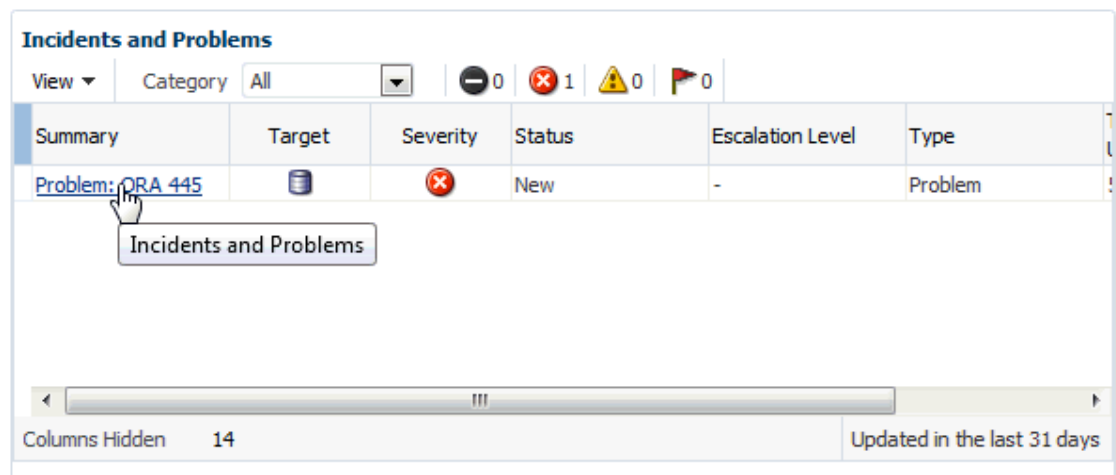


SubSystem	Connections
Availability	0
Configuration	2
Connector Framework	1
Core	2
Event System	2
Enterprise Manager Console	4
Job System	3
Loader	4
Reporting Framework	0
Metadata Service	0

Incidents and Problems

The Incidents and Problems region displays all incidents and problems associated with the repository database. For more detailed incident or problem information, you can click on the **Summary** link to access the issue in Incident Manager.

Figure 1-6 Accessing Incident/Problem Information



Incidents and Problems					
View	Category	All	0	1	0
Summary	Target	Severity	Status	Escalation Level	Type
Problem: ORA 445			New	-	Problem

Columns Hidden 14 Updated in the last 31 days

Initialization Parameter Compliance for Instance

This region displays the current initialization parameter settings, recommended standards, and whether the current parameter values comply with those standard values.

Figure 1-7 Initialization Parameter Compliance

Initialization Parameter Compliance for Instance : semgc12 Instance Name semgc12 semgc12

Enterprise Manager Size **Eval**

Parameter Name	Current Value	Recommended Value	Compliance
pga_aggregate_target	268,435,456	0	✓
open_cursors	300	300	✓
job_queue_processes	20	20	✓
db_block_size	8,192	8,192	✓
sga_target	805,306,368	0	✓
shared_pool_size	314,572,800	471,859,200	✗
processes	300	300	✓
redo log file size	314,572,800	52,428,800	✓

If you are running the repository in a RAC environment, this region also lets you select individual database instances in order to view initialization parameter compliance for that specific instance.

Repository Scheduler Job Status

The **Repository Scheduler Jobs Status** region provides details of the DBMS Jobs regarding their status, duration, and the next scheduled run time.

Figure 1-8 Repository Scheduler Job Status Region

Repository Scheduler Jobs Status Restart Job

DBMS Job Name	Status	Duration	Next Scheduled Run	Edit
Adaptive Threshold Jobs	↑	0.00 s	✓	
Agent Ping	↑	0.06 s	✓	
EM Audit Externalization Se...	↑	0.01 s	✓	
Beacon Service Availability	↑	0.02 s	✓	
Change Activity Planner Ta...	↑	0.21 s	✓	
Cost Based Optimizer Statis...	↑	21.37 s	✓	
Compute Metric Baseline St...	↑	0.09 s	✓	
EM Daily Maintenance	↑	2.89 s	✓	
EM General Purge Policies	↑	1.43 s	✓	
Feature Use Data Collection	↑	2.11 s	✓	

If the **Status** of a job is down, you can run the job again by clicking **Restart Job**.

For high-cost jobs requiring greater resources that, when run, can reduce repository performance, an edit icon (pencil) appears in the **Edit** column. Clicking on the icon displays a dialog allowing you to reschedule the next run time.

Figure 1-9 Job Reschedule Dialog

Schedule Next Run: Adaptive Threshold Extract and Compute Job Job X

Next Scheduled Run Dec 4, 2024 2:00:00 AM GMT

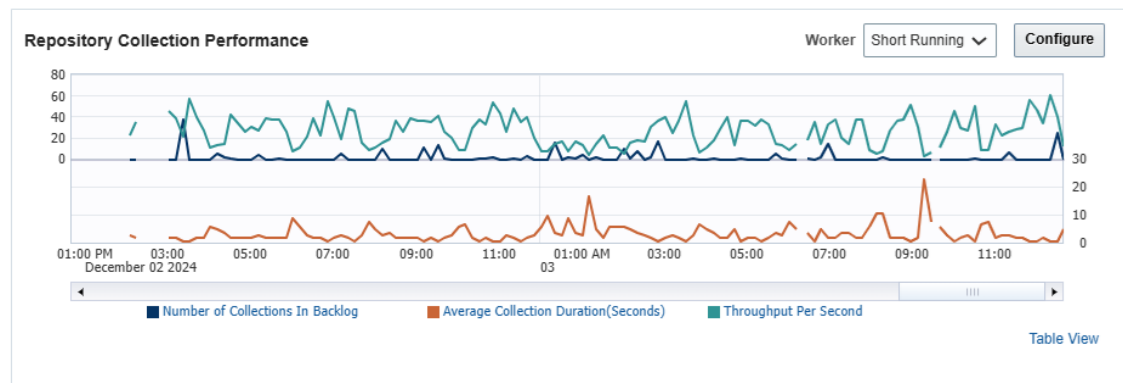
Reschedule To: Hr: 12 Min: 0 ☒ AM ☐ PM

Save Cancel

Repository Collection Performance

The Repository Collection Performance region provides information on the performance of repository collections. They are collected by background DBMS jobs in the repository database called collection workers.

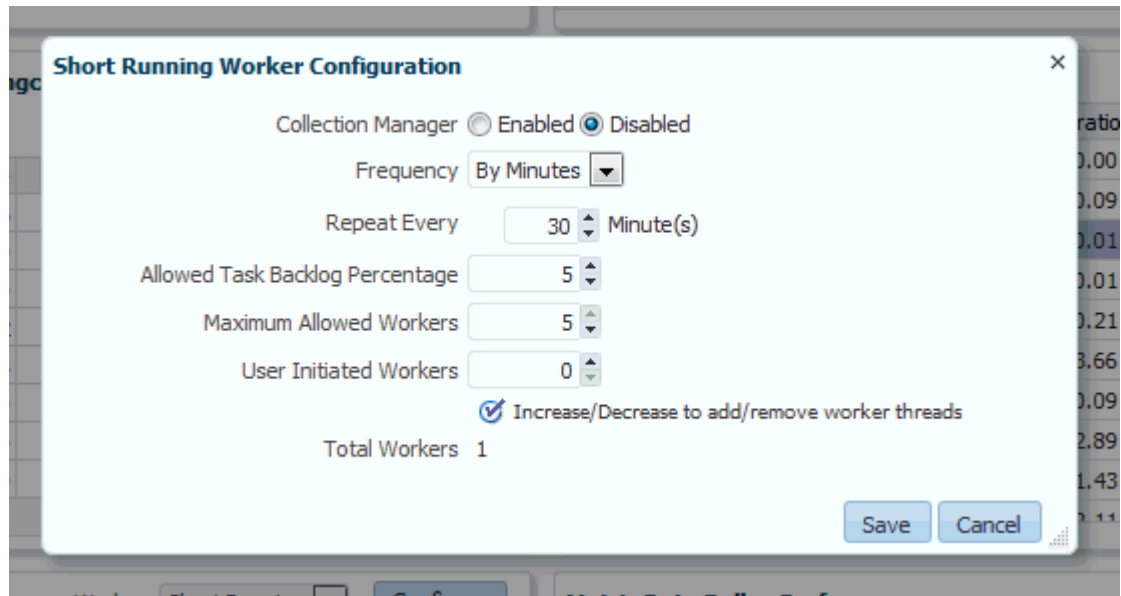
Figure 1-10 Repository Collection Performance Region



Repository metrics are sub-divided into long and short running metrics. These are called task classes (short task class and long task class). Some collection workers process the short task class and some process long task class. Repository collection performance metrics measure the performance data for repository metric collections for each task class. This metric is a repository metric and hence collected by the collection workers.

You can select between **Short Running** and **Long Running** collection workers. When viewing Short Running workers, you can click **Configure** to change short worker settings.

Figure 1-11 Short Worker Configuration Dialog



Short Running Worker Configuration

Collection Manager ☐ Enabled ☒ Disabled

Frequency ▾

Repeat Every Minute(s)

Allowed Task Backlog Percentage

Maximum Allowed Workers

User Initiated Workers

☒ Increase/Decrease to add/remove worker threads

Total Workers 1

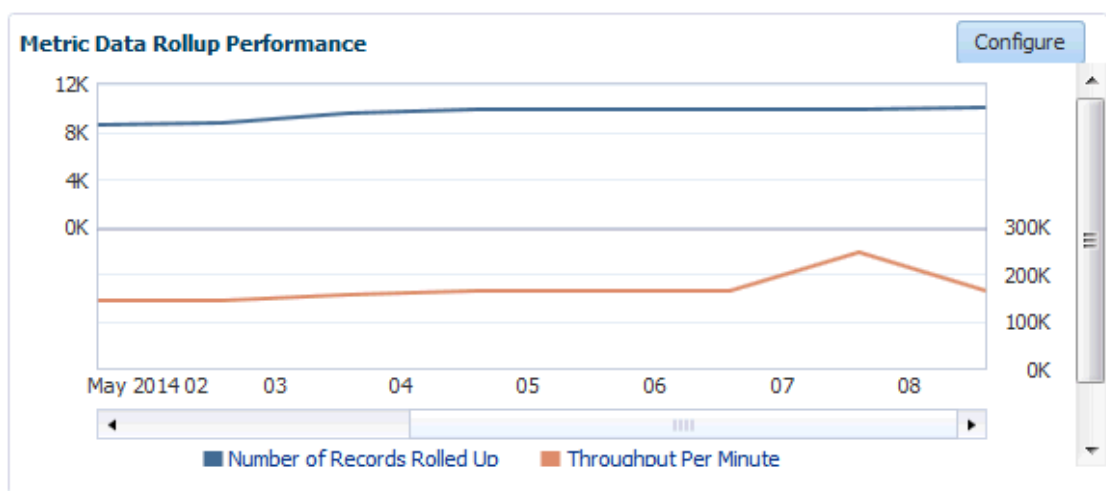
Clicking **Save** submits a job to change the worker configuration. For this reason, the change will not be instantaneous and may require a minute or so in order to take effect.

Clicking on an item in the legend allows you to drill down into Problem Analysis, Metric Details, or the Target Home.

Metric Data Rollup Performance

This region displays the rollup performance by graphically displaying the quantity of data being rolled up (Number of Records Rolled Up) and speed (Throughput per Minute) over time.

Figure 1-12 Metric Data Rollup Performance Region



The graphs for *Number of Records Rolled Up* and *Throughput per Minute* may increase over time as more targets are added, but on a daily basis should remain about the fairly level. Large spikes could indicate that agents are not communicating properly to the OMS

Clicking **Configure** allows you to change the number of rollup worker threads that will be started.

Metrics Tab

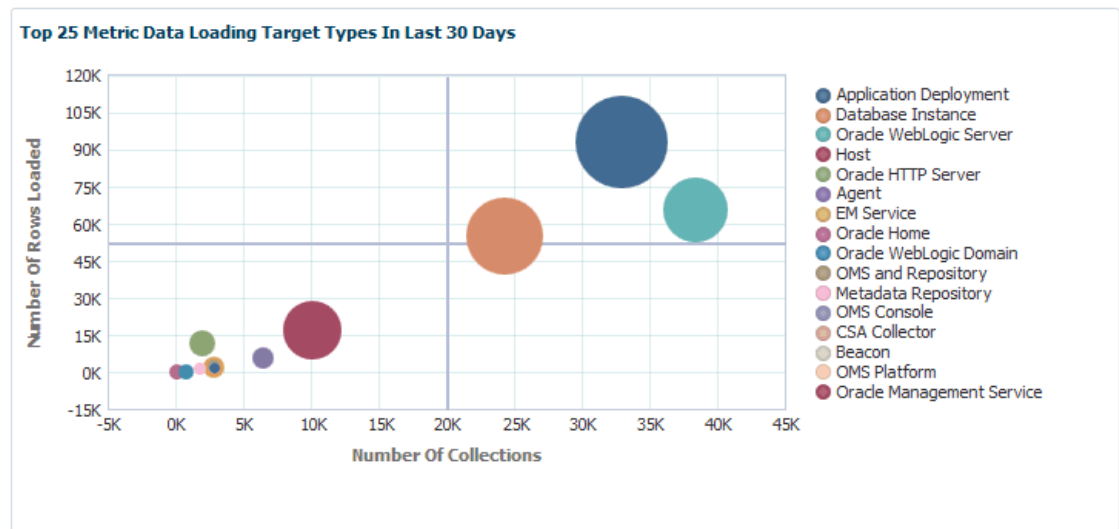
The Metrics tab provides a graphical rollup of key repository performance measurements. Information includes:

- Top 25 Metric Data Loading Target Types In Last 30 Days
- Top 10 Data Loading Metrics In Last 30 Days
- Metric Alerts Per Day In Last 30 Days
- Top 10 Metric Collection Errors By Target Type In Last 30 Days

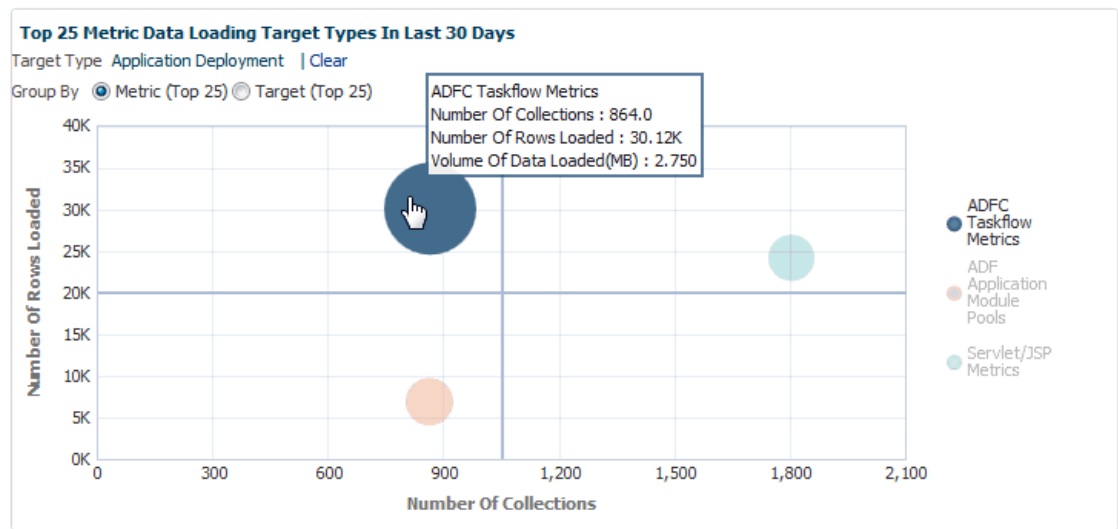
The graphs allow you to drill down to access information in greater detail.

Top 25 Metric Data Loading Target Types In Last 30 Days

Figure 1-13 Top 25 Metric Data Loading Target Types In Last 30 Days

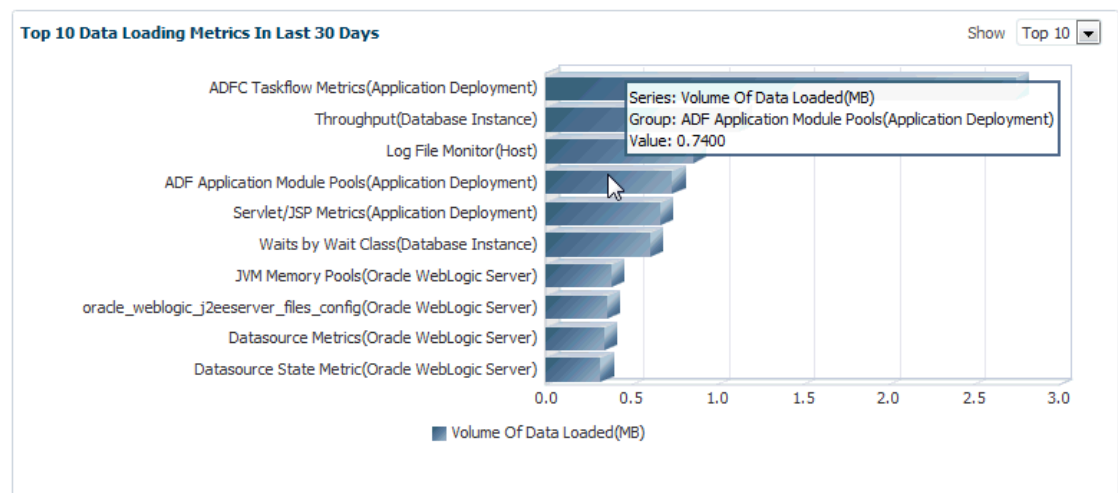


If you wish to view only metrics for a specific target type, click on a specific metric target type area within the graph. A new graph displays showing only metrics for that specific target type. You have the option grouping the results by metric or target.

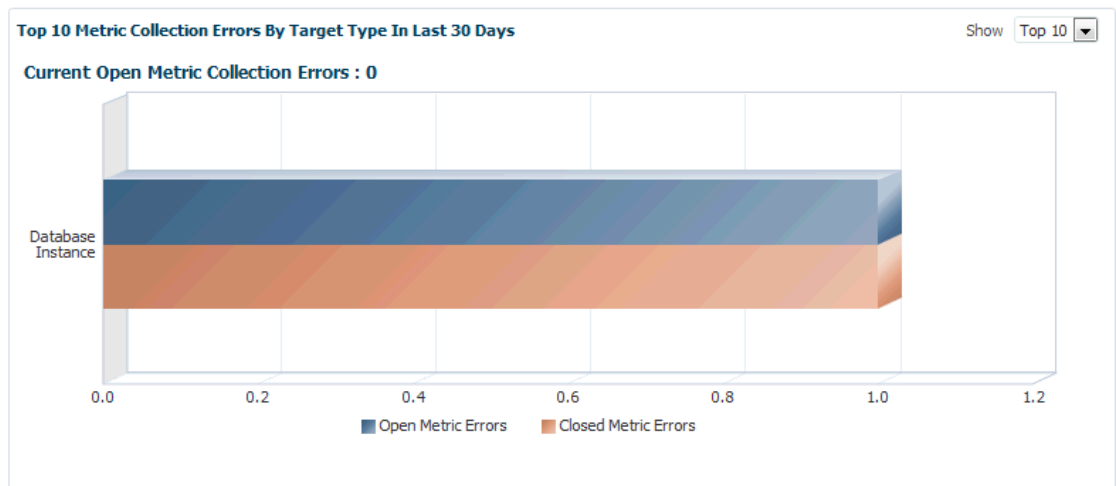
Figure 1-14 Top 25 Metric Data Loading for a Single Target Type

Click **Clear** to return to the original graph containing all target types.

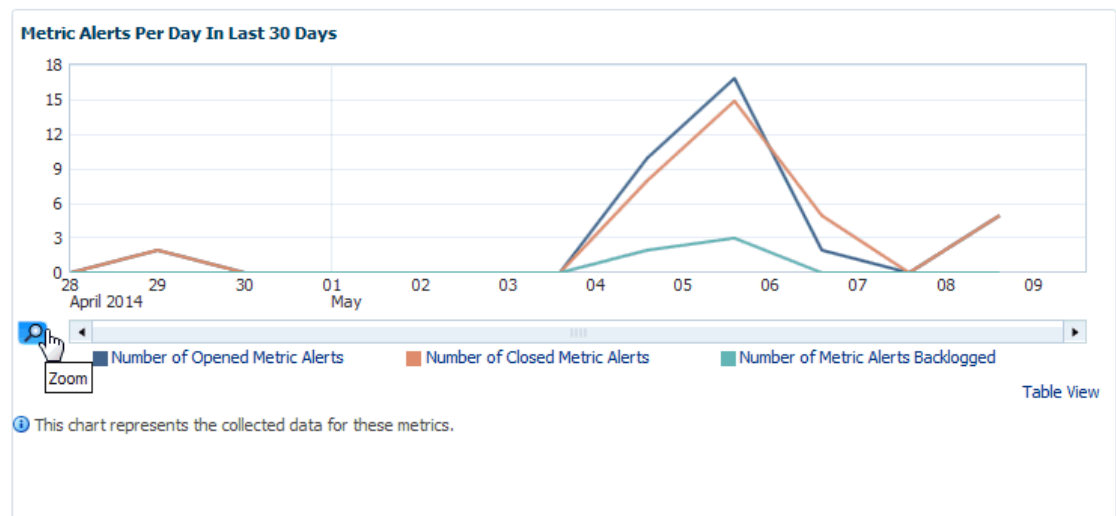
Top 10 Data Loading Metrics In Last 30 Days

Figure 1-15 Metric Data Load Volume

Top 10 Metric Collection Errors By Target Type In Last 30 Days

Figure 1-16 Open Metric Collection Errors**Metric Alerts Per Day In Last 30 Days**

The Metric Alerts Per Day In Last 30 Days graphically displays the number of open, closed, and backlogged metric alerts over time. If you wish to focus on a narrower time span, click **Zoom**.

Figure 1-17 Metric Alerts Per Day

Schema Tab

The Schema tab provides physical attribute and performance data pertaining to the repository database schema. Information includes:

- Tablespace Growth Rate

You can select the specific tablespace: MGMT_TABLESPACE, MGMT_ECM_DEPOT_TS, or MGMT_AD4J_TS. Top 20 Large Tables/Indexes are also displayed.

- Top 20 Tables with Unused Space in Repository
- Purge Policies
- Partition Retention

Controlling and Configuring Management Agents

You can manage Management Agents directly from the Enterprise Manager console. This provides a central point where all the Management Agents within your monitored environment can be compared, configured and controlled.

Manage Agents Page

The Agents page lists all Management Agents within your monitored environment. This page also includes misconfigured, blocked and both upgradable and non- upgradable Agents.

Accessing the Agent Page

From the **Setup** menu, select **Manage Enterprise Manager** and then **Agents**.

Misconfigured and Blocked Agents

A *misconfigured* Agent is an Agent that is not able to perform a heartbeat or upload data to the Oracle Management Service (OMS) due to invalid configuration or invalid data. Agent misconfiguration alerts are triggered by the following metrics:

- Consecutive metadata upload failure count
- Consecutive ping failure count
- Consecutive severity upload failure count
- OMS Agent time skew

If the Agent heartbeat or upload requests are failing consistently, and the problem cannot be resolved in a timely manner, you can manually *block* the Agent to prevent excessive load on the OMS. When you block an Agent, the OMS rejects all heartbeat or upload requests from the blocked Agent. However, even though blocked Agents continue to collect monitoring data, it will not be able to upload any alerts or metric data to the OMS. Once the Agent configuration problem is resolved, you must manually *unblock* the Agent to resume normal operation.

Note

Before unblocking the Agent, ensure that all issues related to Agent misconfiguration have been resolved.

From this page, you can also initiate the Agent upgrade process. For more information about upgrading Agents, see [Upgrading Multiple Management Agents](#).

Agent Home Page

The Agent home page provides details for a single Agent. This page also lets you drill down for more detailed information. You can access an Agent home page by clicking on a specific Agent from in the Agent list page or by selecting it from the All Targets page.

- The **Summary** region provides primary details of the Agent such as its status and availability. The Interaction with Management Service region provides details on the communication between the OMS and the Agent and metric extensions and management plug-ins deployed in the Agent.
- The **Status** region provides further details on the Agent status such as the number of restarts, the action that the Agent is performing currently.
- The **Performance, Usage and Resource Consumption** charts provide further details on the Agent in graphical format.
- The **Incidents** region lists the incidents recorded for the Agent.
- The **Monitoring** region provides details on the targets that are being monitored by the Agent. You can filter targets in this region by All, Broken, and Not Uploading. Separate tabs within the Monitoring section display Metric Issues and Top Collections.

Controlling a Single Agent

Control operations for a single Agent can be performed on the Agent home page for that Agent.

1. Navigate to the desired Agent home page.
2. From the **Agent** drop-down menu, choose **Control** and then one of the control operations (Start Up/Shut Down, or Restart)

Note

You must have at least operator privileges in order to perform Agent control operations.

Upon choosing any of the above control menu options, a pop-up dialog requesting the credentials of the user displays. These operations require the credentials of the OS user who owns the Agent, or credentials of a user who has SUDO or PowerBroker privilege of the Agent owner. At this point, you can either choose from a previously stored username/password, preferred or named credential. You also have the option of choosing a new set of credentials which could also be saved as the preferred credential or as a named credential for future use.

Once you are authenticated, the chosen control operation begins and continues even if the pop-up dialog is closed. Any message of failure/success of the task is displayed in the pop-up dialog.

When choosing the Secure/Resecure/Unsecure options, you must provide the requisite Registration Password.

Agent Control When Using a Server Load Balancer

When choosing the Agent Secure/Resecure options in a multi-OMS environment with a server load balancer (SLB), the Agent will be secured/resecured against the SLB automatically without administrator intervention.

Configuring Single Management Agents

Configuration operations for a single Agent can be performed from the Agent home page. To access the Agent properties page:

1. Navigate to the desired Agent home page.

2. From the **Agent** drop-down menu, select **Properties**.

Note

You must have at least *Configure* privileges in order to perform Agent configuration operations.

The properties on this page can be filtered to show **All Properties**, **Basic Properties**, or **Advanced Properties**. The **Basic Properties** are a simple name, value combination of a property and its value. **Advanced Properties** are also a combination of name and value but can also be grouped into categories. You must have at least *configure* privileges in order to modify the existing properties and set custom properties.

Controlling Multiple Management Agents

In order to perform control operations on multiple Management Agents, Enterprise Manager makes use of the Job system to automate repetitive tasks. Therefore, you must have Job privileges for controlling multiple Management Agents through a single action. To access

1. From the **Setup** menu, select **Manage Enterprise Manager** and then **Agents**. The Agent page displays.
2. Select multiple Management Agents from the list.
3. Click one of the control operation buttons (**Start Up/Shut Down/Restart/Secure/Resecure/Unsecure**).

When you click on any of the control operations, you are taken to the Job creation wizard where you schedule a new job to perform the action on the selected Agents.

In the Jobs page, you can view the chosen Management Agents in Target section in the General tab. You can add more Management Agents by clicking the **Add** button. You then provide the parameters for the operation in the **Parameters** tab, if needed. The credentials must be specified in the **Credentials** tab where you can either choose from a previously stored username/password, preferred, or named credential. You also have the option of choosing a new set of credentials which could also be saved as the preferred credential or as a named credential for future use. You are given the option to start the job immediately or schedule the job for a later time. At this point, you can also create a repeating job by specifying the job start time, the frequency, and the end time.

The Access tab displays the Administrator details and the access levels they have to the job. You can then add a new administrator or modify the access level to **View** or **Full**, if you have the requisite privileges.

Note

Administrators with insufficient privileges can also schedule jobs for these control operations, but in this situation, the jobs will not complete successfully.

Configuring Multiple Agents

As with multi-Agent control operations, you can also perform Agent configuration on multiple Agents in the same way. This greatly simplifies standardizing Agent configurations across your enterprise. To access Agent properties:

1. From the **Setup** menu, select **Manage Enterprise Manager** and then **Agents**. The Agents page is displayed.
2. Select multiple Management Agents from the list.
3. Click **Properties**. As with any multi-Agent operation, configuration is implemented using the Job system.

In the **Create 'Agents Configuration Operation' Job** page, you can view the chosen Management Agents in the Target section of the General tab. You can add more Management Agents by clicking the **Add** button if necessary. In the **Parameters** tab, you provide the modified value for a particular set of properties that you want to change. You can also set a custom property for the chosen agents. No credentials are required for modifying Agent properties.

The **Access** tab displays the administrator details and the access levels they have to the job. You can then add a new administrator or modify the access level to View or Full if you have the requisite privileges.

Upgrading Multiple Management Agents

When you upgrade to the current Enterprise Manager release, you upgrade your Oracle Management Services (OMS) to the current release, but not your target Oracle Management Agents (Management Agents). To mass-upgrade your Management Agents, access the Upgrade Agents page. To access this page:

1. From the **Setup** menu, select **Manage Enterprise Manager**, then select **Agents**.
2. Click **Upgradable**, then select the Management Agents you want to upgrade.
3. Click **Upgrade**.

Alternatively, to access the Upgrade Agents page, from the **Setup** menu, select **Manage Enterprise Manager**, then select **Upgrade Agent**. For more information on upgrading Management Agents, see Upgrading Oracle Management Agents.

Management Servers

A Management Server is a composite target consisting of multiple Enterprise Manager Management Services.

The Management Servers page displays the list of Management Services, their status, incidents, the loader throughput, CPU usage, and the JVM memory usage metrics. In addition, the Management Services displayed can be filtered by Normal Mode, Console Only, PBS only and Standby Management Services.

Accessing the Management Servers Page

From the **Setup** menu, select **Manage Enterprise Manager** and then **Management Servers**.

This page consists of the following sections:

- **Summary:** Displays the high-level information about WebLogic administration server and Load balancer.
- **Job System:** Displays information about the status of jobs over past time periods (such as the last 30 minutes, 1 hour, or 2 hours).
- **Servers:** Displays information about individual Management Services of the Management Server.

- **Loader:** Displays information that provides insight into the Loader subsystem performance as a whole.

There are primarily 3 graphs as follows.

- **Throughput (Rows processed per second):** Indicates the rate (rows processed per second) at which the Loader is processing files.
- **Files Processed vs Backoff:** Indicates the number of files processed versus backed off (rejected) by the Loader. Note: You should contact Oracle Support if consistent backoffs are being generated.
- **% Utilized Capacity:** Shows the current Loader CPU utilization. If the Loader consistently runs at more than 85% capacity, contact Oracle Support to confirm whether your system capacity needs to be increased.

To view detailed IP reports of Loader statistics, click the **Loader Statistics** link located below the graphs.

- **Incidents:** This displays the incidents and problems that have occurred against individual targets hosting Management Services.

Job System Diagnostics

Many factors can impact Job System performance such as user-suspended jobs or long-running jobs blocking resources. The Job System diagnostics dashboard provides insight into the operations and performance of the Job System, thus allowing you to diagnose and resolve any job-related issues quickly.

For more information about the Job System diagnostics dashboard and factors that can affect Job System performance, see *Diagnosing Job System Issues* and *Accessing Job Diagnostics*.

Compliance Standards

Sizing compliance standards rules are built into Enterprise Manager. By default, Enterprise Manager checks the Enterprise Manager repository target against these rules and will send alerts suggesting changes for optimal performance.

The *Enterprise Manager Sizing* compliance standard consists of the following compliance rules:

- Enterprise Manager Minimum Hardware and Storage Requirements
- Enterprise Manager Minimum Database Setting Requirements
- Enterprise Manager Tuning Setting Requirements

To view the Enterprise Manager Sizing Compliance Standard:

1. From the Enterprise menu, select **Compliance** and then **Results**. The Compliance Results page displays with the Evaluation Results table shown.
2. In the Compliance Standards column, click **Enterprise Manager Sizing** compliance standard. The Enterprise Manager Sizing compliance results page displays.

2

Maintaining and Troubleshooting the Management Repository

This section describes maintenance and troubleshooting techniques for maintaining a well-performing Management Repository.

Specifically, this chapter contains the following sections:

- [Management Repository Deployment Guidelines](#)
- [Management Repository Data Retention Policies](#)
- [Dropping and Recreating the Management Repository](#)
- [Troubleshooting Management Repository Creation Errors](#)
- [Cross Platform Enterprise Manager Repository Database Migration](#)

Management Repository Deployment Guidelines

To be sure that your management data is secure, reliable, and always available, consider the following settings and configuration guidelines when you are deploying the Management Repository:

- Install a RAID-capable Logical Volume Manager (LVM) or hardware RAID on the system where the Management Repository resides. At a minimum the operating system must support disk mirroring and striping. Configure all the Management Repository data files with some redundant configuration.
- Use Real Application Clusters to provide the highest levels of availability for the Management Repository.
- If you use Enterprise Manager to alert administrators of errors or availability issues in a production environment, be sure that the Enterprise Manager components are configured with the same level of availability. At a minimum, consider using Oracle Data Guard to mirror the Management Repository database. Configure Data Guard for zero data loss. Choose between Maximum Availability or Maximum Protection based on your environment and needs.
- Oracle strongly recommends that archive logging be turned on and that a comprehensive backup strategy be in place prior to an Enterprise Manager implementation going live in a production environment. The backup strategy should include archive backups and both incremental and full backups as required.

See Also

Installation of Enterprise Manager in the *Oracle Enterprise Manager Installation and Basic Configuration* guide for information about the database initialization parameters required for the Management Repository

- Oracle recommends that you not use SQL Plan Management (SQL plan baselines and capture) with the Enterprise Manager repository. If you do need to use it for a specific

problem, shut it off immediately after using. Issues with the Enterprise Manager repository may occur when using SQL Plan Management, such as very poor SQL performance using unverified plans, and deadlocks between SQL Plan Management capture and the Enterprise Manager security VPD.

- After enabling auditing for the repository database and for audit entries related to ORA-errors, error messages should be ignored if they are not reported in the Enterprise Manager application logs; for example, `emoms.trc`, the `MGMT_SYSTEM_ERROR_LOG` table, or in the `alert.log` of the repository database. In these cases the errors are harmless.
- To see a list of the regular maintenance activities that need to be performed for the repository, see the Sizing Your Enterprise Manager Deployment in the *Oracle® Enterprise Manager Advanced Installation and Configuration Guide*.
- To monitor the repository database activities using the Enterprise Manager user interface, see [Maintaining Enterprise Manager](#).
- The Exadata and Recovery Appliance fleet pages and the features of the Exadata and Zero Data Loss Recovery Appliance Management Packs require Oracle Text to be installed on the Enterprise Manager repository database. For information on how to install Oracle Text, see *Oracle Text Installation Steps For New 19c Installs* (Doc ID 2591868.1) in [My Oracle Support](#).
- If creating multiple PDBs in a CDB as separate Enterprise Manager repositories, for example individual PDBs as repositories for multiple Enterprise Manager sites, you must use a non-SYS user to deploy the Enterprise Manager software. For more details on how to create and use a non-SYS user when installing Enterprise Manager, see Evaluate Non-SYS User Creation in *Enterprise Manager Advanced Installation and Configuration Guide*.
- A Transparent Data Encryption (TDE) enabled repository is supported when installing, patching, or upgrading Enterprise Manager.

Management Repository Data Retention Policies

When the various components of Enterprise Manager are configured and running efficiently, the Oracle Management Service gathers large amounts of raw data from the Management Agents running on your managed hosts and loads that data into the Management Repository. This data is the raw information that is later aggregated, organized, and presented to you in the Enterprise Manager console.

After the Oracle Management Service loads information into the Management Repository, Enterprise Manager aggregates and purges the data over time.

The following sections describe:

- The default aggregation and purging policies used to maintain data in the Management Repository.
- How you can modify the length of time the data is retained before it is aggregated and then purged from the Management Repository.

Management Repository Default Aggregation and Purging Policies

Enterprise Manager aggregates collected metric data by hour and by day to enhance query performance and help minimize the size of the Management Repository. Before the data is aggregated, each data point is stored in a raw metric data table. Once a day, the previous day's raw metric data is rolled up, or aggregated, into a one-hour and a one-day table. These hourly and daily records will have hourly and daily metric data averages, minimums, maximums and standard deviations respectively.

After Enterprise Manager aggregates the data, the data is then considered eligible for purging. A certain period of time must pass for data to actually be purged. This period of time is called the retention time.

The raw data, with the highest insert volume, has the shortest default retention time, which is set to 7 days. As a result, 7 days after it is aggregated into a one-hour record, a raw data point is eligible for purging.

Note

This data retention policy varies for JVMD and ADP data.

Hourly aggregate metric data records are purged after 32 days. The highest level of aggregation, one day, is kept for 24 months (roughly 730 days).

The default data retention policies are summarized in [Table 2-1](#).

Table 2-1 Default Repository Purging Policies

Aggregate Level	Retention Time
Raw metric data	7 days
Hourly aggregated metric data	32 days
Daily aggregated metric data	24 months

If you have configured and enabled Application Performance Management, Enterprise Manager also gathers, saves, aggregates, and purges response time data. The response time data is purged using policies similar to those used for metric data. The Application Performance Management purging policies are shown in [Table 2-2](#).

Table 2-2 Default Repository Purging Policies for Application Performance Management Data

Aggregate Level	Retention Time
Raw response time data	24 hours
One-hour aggregated response time data	7 days
One-hour distribution response time data	24 hours
One-day aggregated response time data	32 days
One-day distribution aggregated response time data	32 days

If you do not want to keep severity data for the default period (6 months), and want to reduce the retention period for the EVENTS purge policy, you can use the following command:

```
em_purge.modify_purge_policy_group('EVENTS',NULL,*1_new_purge_hours*);
```

This command will modify only the purge policy group which will affect all the purge policies associated with that group. Note that if a purge policy is associated with a purge group, the

retention period is taken as the retention period of the group. When the retention of a purge policy (associated with a purge policy group) is changed, then the retention is determined from the purge policy and not from the purge policy group.

To modify an individual purge policy use the following command:

```
em_purge.modify_purge_policy(  
    p_policy_name      IN VARCHAR2,  
    p_retention_hours  IN NUMBER  
)
```

You can modify the purge policy and also the partition retention values by choosing **Manage Enterprise Manager** from the **Setup** menu, then selecting **Repository**. From that page, choose the Schema tab and then make any necessary changes in the Purge Policies section (click **Modify**) or Partition Retention section.

Events data is partitioned and maintains six months of historical data by default. You can change the default retention period using the procedure described above. The severity data is tied to the events data purge policy and will be adjusted accordingly.

The fixed set of tables affected by this data purge are listed below:

```
EM_EVENT_SEQUENCES  
EM_EVENT_RAW  
EM_EVENT_MSGS  
EM_EVENT_CONTEXT  
EM_EVENT_ANNOTATIONS  
EM_EVENTS_INCIDENT  
EM_ISSUES_INTERNAL  
EM_ISSUES_MSG  
EM_ISSUES_ANNOTATIONS  
EM_INCIDENT_ISSUE  
EM_PROBLEM_ISSUE  
EM_INCIDENTS_PROBLEM
```

The following list is a dynamic set of tables that store data for different event types supported by Enterprise Manager. This list can vary over time as new event types or unsupported event types are added or removed:

```
EM_EV_CS_RULE_VIOLATION  
EM_EV_CS_SCORE  
EM_EV_JOB_STATUS_CHANGE  
EM_EV_METRIC_ALERT  
EM_EV_METRIC_ERROR  
EM_EV_MEXT_UPDATE  
EM_EV_MNTR_DISRUPTION  
EM_EV_SELFUPDATE  
EM_EV_SLA_ALERT  
EM_EV_TARGET_AVAILABILITY  
EM_EV_USER_REPORTED  
EM_EV_ADP_ALERT  
EM_EV_APM_KPI_ALERT  
EM_EV_JVMDIAG_ALERT  
EM_EV_HA_EVENT
```

Management Repository Default Aggregation and Purging Policies for Other Management Data

Besides the metric data and Application Performance Monitoring data, other types of Enterprise Manager data accumulates over time in the Management Repository.

For example, the last availability record for a target will also remain in the Management Repository indefinitely, so the last known state of a target is preserved.

Modifying the Default Aggregation and Purging Policies

The Enterprise Manager default aggregation and purging policies were designed to provide the most available data for analysis while still providing the best performance and least disk-space requirements for the Management Repository. As a result, you should not modify these policies to improve performance or increase your available disk space.

However, if you plan to extract or review the raw or aggregated data using data analysis tools other than Enterprise Manager, you may want to increase the amount of raw or aggregated data available in the Management Repository. You can accomplish this by increasing the retention times for the raw or aggregated data.

A PL/SQL API has been provided to modify the default retention time for the core metric data tables in the Enterprise Manager repository. [Table 2-3](#) shows the default number of partitions retained for each of the three tables and the size of the partitions for each table. The API will allow you to change the number of partitions retained only.

Table 2-3 Core EM Metric Data Tables and Default Data Retention in the Management Repository

Table Name	Partitions Retained	Partition Size
EM_METRIC_VALUES_E	7	DAY
EM_METRIC_VALUES_HOURLY_E	32	DAY
EM_METRIC_VALUES_DAILY_E	24	MONTH

To modify the retention period for any of the above tables, execute the following command:

```
SQL> execute gc_interval_partition_mgr.set_retention('SYSMAN', <table name>,
<number of partitions to retain>);
```

Replace the <table name> by name of table as listed above. The API will allow you to change the number of partitions retained only.

For example, to modify the default retention time for the table EM_METRIC_VALUES_E from 7 partitions to 14 partitions, follow these steps:

1. Use SQL*Plus to connect to the repository database as the SYSMAN user.
2. Check the current value of the retention periods:

```
SQL> select table_name, partitions_retained
from em_int_partitioned_tables
where table_name in
('EM_METRIC_VALUES_E', 'EM_METRIC_VALUES_HOURLY_E', 'EM_METRIC_VALUES_DAILY_E');
```

```
TABLE_NAME                PARTITIONS_RETAINED
-----
EM_METRIC_VALUES_E                7
EM_METRIC_VALUES_HOURLY_E        32
EM_METRIC_VALUES_DAILY_E        24
```

3. To modify the default retention time for the table EM_METRIC_VALUES_E from 7 partitions to 14, execute the following command:

```
SQL> execute gc_interval_partition_mgr.set_retention('SYSMAN',
'EM_METRIC_VALUES_E', 14);
```

4. Verify that the retention period has been modified:

```
SQL> select table_name, partitions_retained
from em_int_partitioned_tables
where table_name in
('EM_METRIC_VALUES_E', 'EM_METRIC_VALUES_HOURLY_E', 'EM_METRIC_VALUES_DAILY_E');
```

TABLE_NAME	PARTITIONS_RETAINED
EM_METRIC_VALUES_E	14
EM_METRIC_VALUES_HOURLY_E	32
EM_METRIC_VALUES_DAILY_E	24

How to Modify the Retention Period of Job History

Enterprise Manager has a default purge policy which removes all finished job details which are older than 30 days. This section provides details for modifying this default purge policy.

The actual purging of completed job history is implemented via a DBMS_SCHEDULER job that runs once a day in the repository database. When the job runs, it looks for finished jobs that are 'n' number of days older than the current time (value of sysdate in the repository database) and deletes these jobs. The value of 'n' is, by default, set to 30 days.

The default purge policy cannot be modified via the Enterprise Manager console, but it can be changed using SQL*Plus.

To modify this purge policy, follow these steps:

1. Log in to the repository database as the SYSMAN user, via SQL*Plus.
2. Check the current values for the purge policies using the following command:

```
SQL> select * from mgmt_job_purge_policies;
```

POLICY_NAME	TIME_FRAME
SYSPURGE_POLICY	30
REFRESHFROMMETALINKPURGEPOLICY	7
FIXINVENTORYPURGEPOLICY	7
OPATCHPATCHUPDATE_PAPURGEPOLICY	7

The purge policy responsible for the job deletion is called SYSPURGE_POLICY. As seen above, the default value is set to 30 days.

3. To change the time period, you must drop and recreate the policy with a different time frame:

```
SQL> execute MGMT_JOBS.drop_purge_policy('SYSPURGE_POLICY');
```

PL/SQL procedure successfully completed.

```
SQL> execute MGMT_JOBS.register_purge_policy('SYSPURGE_POLICY', 60, null);
```

PL/SQL procedure successfully completed.

```
SQL> COMMIT;
```

Commit complete.

```
SQL> select * from mgmt_job_purge_policies;
```

POLICY_NAME	TIME_FRAME
-------------	------------

SYSPURGE_POLICY

60

....

The above commands increase the retention period to 60 days. The time frame can also be reduced below 30 days, depending on the requirement.

You can check when the purge job will be executed next. The actual time that the purge runs is set to 5 AM repository time and can be verified using these steps:

1. Login to the Repository database using the SYSMAN account.
2. Execute the following command:

```
SQL> select job_name,
           to_char(last_start_date, 'DD-MON-YY HH24:MI:SS') last_run,
           to_char(next_run_date, 'DD-MON-YY HH24:MI:SS') next_run
from all_scheduler_jobs
where job_name = 'EM_JOB_PURGE_POLICIES';
```

JOB_NAME	LAST_RUN	NEXT_RUN
EM_JOB_PURGE_POLICIES		07-SEP-11 05:00:00

The schedule can also be verified from the Enterprise Manager console by following these steps:

- a. From the **Setup** menu, select **Management Service**, then select **Repository**.
- b. Click the **Repository Operations** tab.
- c. Find the Next Scheduled Run and Last Scheduled Run information for Job Purge in the list.

Please note that the time of the next scheduled execution of the Job Purge does not represent the cutoff time for the retention period; the cutoff time is determined by the purge policy at the time the Job Purge runs.

DBMS_SCHEDULER Troubleshooting

Enterprise Manager uses the database scheduler (dbms_scheduler) to run various processes in the repository. When the dbms_scheduler is stopped or has insufficient resources to operate, the Enterprise Manager processes do not run or are delayed. The following is a list of common causes that may prohibit the dbms_scheduler from running normally.

Job Queue Processes

The dbms_scheduler uses a separate job-queue process for each job it runs. The maximum number of these processes is controlled by the database parameter, *job_queue_processes*. If all processes are in use, no new jobs will be started.

The following query returns the number of currently running jobs.

```
SQL> SELECT count(*)
FROM dba_scheduler_running_jobs;
```

If the count is close to the setting of *job_queue_processes*, it could mean that Enterprise Manager dbms_scheduler jobs cannot be started (on time). Determine if any of the running dbms_scheduler jobs are stuck and consider increasing the setting for *job_queue_processes*.

Job Slave Processes

The `dbms_scheduler` also depends on the setting of the `dbms_scheduler` property `MAX_JOB_SLAVE_PROCESSES`. If the number of running `dbms_scheduler` jobs exceeds this setting, no new jobs will be started. This attribute can be checked using this query.

```
SQL> SELECT value
FROM dba_scheduler_global_attribute
WHERE attribute_name='MAX_JOB_SLAVE_PROCESSES';
```

If the count equals the number of running `dbms_scheduler` jobs, then determine if any of the running `dbms_scheduler` jobs are stuck and consult the `dbms_scheduler` documentation about how to adjust this attribute.

DBMS_SCHEDULER Program Disabled

The `dbms_scheduler` has an attribute that can be set to disable this feature in the database. When set, the Enterprise Manager `dbms_scheduler` jobs will not run. To check if this attribute has been set (inadvertently), run this query.

```
SQL> SELECT *
FROM dba_scheduler_global_attribute
WHERE attribute_name = 'SCHEDULER_DISABLED';
```

When a row is returned, the `dbms_scheduler` is disabled. Execute `dbms_scheduler.set_scheduler_attribute('SCHEDULER_DISABLED', 'FALSE');`

Consult the `dbms_scheduler` documentation about how to remove this attribute.

Too Many Database Sessions

Each `dbms_scheduler` job requires two database sessions. When no more sessions are available, Enterprise Manager `dbms_scheduler` jobs will not run. The following two queries give the maximum number of allowed sessions and the current number of active sessions:

```
SQL> SELECT value
FROM v$parameter
WHERE name='sessions';

SQL> SELECT count(*)FROM v$session;
```

When the current number of sessions approaches the maximum, then you should determine if any of the sessions are stuck and consult the Oracle Database documentation about how to increase the maximum number of sessions.

Also the high water mark of the number of sessions may indicate that this issue has played a role in the past:

```
SQL> select *
from v$resource_limit
where resource_name = 'sessions' ;
```

If the `MAX_UTILIZATION` column indicates a value that is close the maximum number of sessions, it could explain why some of the Enterprise Manager `dbms_scheduler` jobs may not have run (on time) in the past.

Insufficient Memory

The database may not be able to spawn a new job queue process when there is insufficient memory available. The following message in the database alert file, *Unable to spawn jobq slave processes*, in combination with, *(free memory = 0.00M)*, would be indicative of this problem. Please consult the Oracle Database documentation about how to diagnose this memory problem further.

Dropping and Recreating the Management Repository

This section provides information about dropping the Management Repository from your existing database and recreating the Management Repository after you install Enterprise Manager.

It should be noted here that there is no recovery from the drop command so this action is only appropriate if you are decommissioning an Enterprise Manager site.

Dropping the Management Repository

To recreate the Management Repository, you first remove the Enterprise Manager schema from your Management Repository database. You accomplish this task using the `-action drop` argument to the `RepManager` script, which is described in the following procedure.

To remove the Management Repository from your database:

1. Locate the `RepManager` script in the following directory of the Middleware Home where you have installed and deployed the Management Service:

```
ORACLE_HOME/sysman/admin/emdrep/bin
```

Note

Do not use the database version of the `Repmanager` script. It does not delete all components which will result in a failed re-installation.

Also, `RepManager` is the only way to drop the repository, so you should be sure not to delete the OMS Home until the drop has successfully completed.

2. At the command prompt, enter the following command:

```
$PROMPT> RepManager repository_host repository_port repository_SID  
-sys_password password_for_sys_account -action drop
```

In this syntax example:

- `repository_host` is the machine name where the Management Repository database is located
- `repository_port` is the Management Repository database listener port address, usually 1521
- `repository_SID` is the Management Repository database system identifier
- `password_for_sys_account` is the password of the SYS user for the database.
- `-action drop` indicates that you want to drop the Management Repository, MDS, OPSS, APM, and Schemas. If you use `drop`, the command drops only the Management Repository.

Note

The drop command will remove the BI schema (`SYSMAN_BIPLATFORM`) if it exists.

Alternatively, you can use a connect descriptor to identify the database on the RepManager command line. The connect descriptor identifies the host, port, and name of the database using a standard Oracle database syntax.

For example, you can use the connect descriptor as follows to create the Management Repository:

```
$PROMPT> ./RepManager -connect "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=host1)(PORT=1521))) (CONNECT_DATA=(SERVICE_NAME=servicename)))"
-sys_password efkl34lmn -action drop
```

① See Also

"Establishing a Connection and Testing the Network" in the *Oracle Enterprise Manager Licensing Information* for more information about connecting to a database using connect descriptors.

Recreating the Management Repository

The preferred method for creating the Management Repository is to create the Management Repository during the Enterprise Manager installation procedure, which is performed using Oracle Universal Installer.

① See Also

Oracle Enterprise Manager Installation and Basic Configuration for information about installing Enterprise Manager.

In the event a repository is dropped, you cannot create the repository alone using the "RepManager create" command. The command will not create all the required users in the repository database. To create the repository you must completely reinstall Enterprise Manager.

If you are following recommended best practices by regularly backing up the repository, then you can use a backup of the repository as long as any one of the following is true:

- The primary OMS home is intact
- There is an export/config of the primary OMS
- There is a file system back up of the primary OMS

Using a Connect Descriptor to Identify the Management Repository Database

You can use a connect descriptor to identify the database on the RepManager command line. The connect descriptor identifies the host, port, and name of the database using a standard Oracle database syntax.

For example, you can use the connect descriptor as follows to create the Management Repository:

```
$PROMPT> ./RepManager -connect "(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)
(HOST=host1)(PORT=1521))) (CONNECT_DATA=(SERVICE_NAME=servicename)))"
-sys_password efkl34lmn -action create
```

① See Also

"Establishing a Connection and Testing the Network" in the *Oracle Enterprise Manager Licensing Information* for more information about connecting to a database using a connect descriptor

The ability to use a connect string allows you to provide an address list as part of the connection string. The following example shows how you can provide an address list consisting of two listeners as part of the RepManager command line. If a listener on one host becomes unavailable, the second listener can still accept incoming requests:

```
$PROMPT> ./RepManager -connect "(DESCRIPTION=
(AADDRESS_LIST=
(AADDRESS=(PROTOCOL=TCP)(HOST=host1)(PORT=1521)
(AADDRESS=(PROTOCOL=TCP)(HOST=host2)(PORT=1521)
(CONNECT_DATA=(SERVICE_NAME=service_name)))"
-sys_password efkl34lmn -action create
```

Troubleshooting Management Repository Creation Errors

Oracle Universal Installer creates the Management Repository using a configuration step at the end of the installation process. If the repository configuration tool fails, note the exact error messages displayed in the configuration tools window, wait until the other configuration tools have finished, exit from Universal Installer, and then use the following sections to troubleshoot the problem.

Package Body Does Not Exist Error While Creating the Management Repository

If the creation of your Management Repository is interrupted, you may receive the following error when you attempt to create or drop the Management Repository at a later time:

```
SQL> ERROR:
ORA-00604: error occurred at recursive SQL level 1
ORA-04068: existing state of packages has been discarded
ORA-04067: not executed, package body "SYSMAN.MGMT_USER" does not exist
ORA-06508: PL/SQL: could not find program unit being called
ORA-06512: at "SYSMAN.SETEMUSERCONTEXT", line 5
ORA-06512: at "SYSMAN.CLEAR_EMCONTEXT_ON_LOGOFF", line 4
ORA-06512: at line 4
```

To fix this problem, see "[General Troubleshooting Techniques for Creating the Management Repository](#)".

Server Connection Hung Error While Creating the Management Repository

If you receive an error such as the following when you try to connect to the Management Repository database, you are likely using an unsupported version of the Oracle Database:

Server Connection Hung

To remedy the problem, upgrade your database to the supported version as described in *Prerequisites for Installing an Enterprise Manager System in Oracle Enterprise Manager Installation and Basic Configuration*.

General Troubleshooting Techniques for Creating the Management Repository

If you encounter an error while creating the Management Repository, drop the repository by running the `-drop` argument to the `RepManager` script.

See Also

[Dropping the Management Repository](#)

If the `RepManager` script drops the repository successfully, try creating the Management Repository again.

If the `RepManager -action drop/drop` fails for any reason, perform the following steps:

1. Apply the Bundle Patch to the 12c OMS home. Note that this step is only applicable to 12.1.0.1 OMS. Refer to My Oracle Support Note 1393173.1: Enterprise Manager Installation Instructions for Bundle Patch 1 and 12.1.0.2 Plug-ins for instructions.
2. Stop the OMS and verify that all the WLS / OMS processes have been stopped in the OMS home:

```
cd <ORACLE_HOME>/bin
emctl stop oms -all
```

Note

You should use the `-all` option so that the Admin Server is stopped as well

Verify that there are no WLS / OMS processes still running:

```
$ ps -ef | grep EMGC
$ ps -ef | grep java
```

3. Drop the repository objects using the "Repmanager drop" command:

```
cd <ORACLE_HOME>/sysman/admin/emdrep/bin
RepManager <database hostname> <database listener port> <database sid> -action drop -
dbUser sys -dbPassword <sys user password> -dbRole sysdba -mwHome <Middleware Home> -
mwOraHome <Middleware Home> -oracleHome <OMS Home>
```

For example:

```
RepManager repomachine.domain 1521 orcl -action drop -dbUser sys -dbPassword
oracle123 -dbRole sysdba -mwHome /home/oracle/Middleware
-mwOraHome /home/oracle/Middleware -oracleHome /home/oracle/Middleware/oms
```

4. Log in to the Repository Database as `sys` or any DBA user and verify that all the repository objects have been dropped:

```
SQL> select username,account_status from dba_users where username in ('SYSMAN',
'SYSMAN_MDS', 'MGMT_VIEW', 'SYSMAN_BIPLATFORM', 'SYSMAN_APM', 'BIP', 'SYSMAN_OPSS', 'SYSMAN
_RO') ;
```

```
SQL> select owner,synonym_name from dba_synonyms where table_owner in ('SYSMAN',
```

```
'SYSMAN_MDS','MGMT_VIEW','SYSMAN_BIPLATFORM','SYSMAN_APM','BIP','SYSMAN_OPSS','SYSMAN_RO') ;
```

```
SQL> select tablespace_name from dba_tablespaces where tablespace_name like 'MGMT%';
```

```
SQL> select comp_name from SCHEMA_VERSION_REGISTRY;
```

None of the above queries should return any rows. If any of the above queries return any rows, then raise an SR with Oracle Support.

Note

The above solution is applicable if the OMS is in working condition. If the OMS home is not available or not intact, raise an SR with Oracle Support.

Cross Platform Enterprise Manager Repository Database Migration

In the ever evolving data management landscape, businesses frequently encounter the need to migrate databases across different endian platforms. Database migration is a critical operation, often needed due to system upgrades, cloud adoption, or a shift in business requirements. In the context of cross platform and cross endian migration, the challenges are higher as data structures, byte orders, and database formats vary between systems. In the realm of database migration, using Oracle Data Pump technology enables very high-speed movement of data from one database to another across diverse platforms and endian architectures. Whether transitioning between on-premises servers and the cloud, or migrating between different database management systems, a robust data pump mechanism becomes crucial for maintaining data integrity, security, and system performance.

The Enterprise Manager Repository, being the heartbeat of Oracle Enterprise Manager, contains vital metadata and performance data essential for effective monitoring and management of an organization's IT ecosystem. When contemplating a migration across platforms or endian architectures, a meticulous strategy is paramount to ensure the integrity and accessibility of this critical repository.

Data pump technologies play a pivotal role in facilitating the seamless movement of data during these migrations. As we embark on this exploration, this section reviews the complexities of cross platform cross endian migrations within the context of the Enterprise Manager Repository database. It introduces the *RepMigrate* utility and defines the process that can be followed by administrators for successful and reliable migration of the repository database in minimum time and with maximum efficiency.

Oracle recommends using the *RepMigrate* utility for Enterprise Manager repository database migrations.

The overall strategy for migration depends on:

- The source and target database version
- The amount of data and/or size of the repository
- Actual data to migrate

For Oracle database details about cross platform transportable tablespace, data pump, and export/import options, see the [Oracle Database Documentation](#).

Topics:

- [Introduction to RepMigrate](#)
- [How to Get RepMigrate Utility?](#)
- [Repository Migration Steps Using RepMigrate](#)
- [Perform Post Migration Verification](#)
- [RepMigrate Files and Troubleshooting](#)

Introduction to RepMigrate

Oracle recommends using *RepMigrate* utility for Enterprise Manager repository database migration.

RepMigrate is a wrapper utility that is written on top of Oracle Data Pump to ease the cross platform cross endian repository database migration for Enterprise Manager administrators. The utility underlying uses Oracle Data Pump, a feature of Oracle Database since release 10g and successor to the Oracle Export and Import (exp and imp) utilities in release 9i and earlier. Oracle Data Pump is useful for migrating data among schemas, databases of different versions, and on different operating systems, and from on-premises to on-premises and to Oracle Cloud.

How to Get RepMigrate Utility?

Starting with Enterprise Manager 13c Release 5 Update 22 (13.5.0.22), the Release Update file includes the RepMigrate utility (RepMigrate.zip file).

To obtain the **RepMigrate** utility do the following:

1. Download the Release Update file from [My Oracle Support](#) and extract it.
2. After extracting the Release Update, locate the RepMigrate.zip file.
3. Copy the RepMigrate.zip file to the source database.
Copy the file to a location in the repository database host (source database) and unzip it.

Note

You also need to do the same: copy and unzip the file in the target database. The RepMigrate utility version used for the Enterprise Manager repository database migration process must be on the same version as the Enterprise Manager Release Update (RU) deployed.

4. After unzipping the file, you can see the RepMigrate utility directory that you can use for the repository database migration process during the export and import steps as explained in the next sections.

To learn more about RepMigrate parameters, see [RepMigrate Usage](#).

RepMigrate Usage

Starting with Enterprise Manager 13c Release 5 Update 22 (13.5.0.22), the *RepMigrate* utility is included in the Release Update file and available for performing Enterprise Manager repository database migration.

To list all the RepMigrate available options, run:

```
./RepMigrate.sh -help
```

List of Some Useful Parameters:

- `-datafileLocation`: Specifies the datafile options.
This is a mandatory parameter for ASM and RAC environments.
- `-encryptionPassword`: Specifies the password of the encrypted column data, metadata, or table data in the export dump file of the source database for TDE environment.
Ensure to pass the same password during the import operation in the target database.
- `-parallel`: Specifies the maximum number of processes of active execution operating on behalf of the export and/or import job.
- `-prereqOnly`: Specifies to run only the RepMigrate prerequisites check during the export operation. For details, see [Step 3. Run Prerequisites Check](#).
- `-ignorePrereqList`: Ignores the prerequisites check.
- `-repmigrate_prereq_dbpatch`: Checks if the database patch has been applied or not.

For RAC environment, use the connect string-based connection on the first node for the RAC setup. Scan address is not supported.

For SSL configured repository, use `RepMigrate.sh -help` to review the options available.

The *RepMigrate* utility checks for `TEMP` and `UNDO` tablespaces. If there's not enough space available, it will fail.

Repository Migration Steps Using RepMigrate

The following sections discuss the steps for repository migration using RepMigrate utility:

- [Step 1. Prepare Databases](#)
- [Step 2. Best Practices](#)
- [Step 3. Run Prerequisites Check](#)
- [Step 4. Perform Migration](#)

Step 1. Prepare Databases

Complete the following prerequisites to migrate the repository database using RepMigrate:

- [Step 1.1. Perform Common Prerequisites for Source and Target Databases](#)
- [Step 1.2. Complete Source Database Prerequisites](#)
- [Step 1.3. Complete Target Database Prerequisites](#)
- [Step 1.4. Perform Common Prerequisites for Source and Target Enterprise Manager Hosts](#)

Step 1.1. Perform Common Prerequisites for Source and Target Databases

The following lists the prerequisites for both the *source* and *target* databases when using *RepMigrate* utility for repository migration:

- [Database Patches Prerequisites](#)

- [Timezone Prerequisite](#)
- [Tablespace Considerations](#)
- [Other Recommendations](#)

Database Patches Prerequisites

Apply all the database patches to both the *source* and *target* databases as necessary.

Note

Both databases, source and target, should be at the same Database Release Update (DB RU) version with all the patches applied.

- Install the database patch 30978304 on both source and target databases before starting the repository migration process. For database patch information, see [My Oracle Support](#).
- Apply the recommended Oracle Database 19 Release Update 19 (19.19) patches.

Note

Some database patches may be included as part of the Database Release Update (DB RU) patches. Oracle recommends to check if the database patches are listed in your inventory. If you are missing database patches, check [My Oracle Support](#) and see if they are available. If database patches are not available for their release update (RU), you may need to request a one-off patch.

Oracle Database 19 Release Update 19 (19.19) patches:

- Patch 35042068: Database Release Update : 19.19.0.0.230418 (35042068)
- Patch 35261302: DATAPUMP BUNDLE PATCH 19.19.0.0.0

Oracle Database 19 Release Update (RU) patches specific to RU19 and the Data Pump utility:

- Patch 36205997: MAX PGA LIMIT FLAG RESET IN 19C.
- Patch 36018313: MERGE ON DATABASE RU 19.19.0.0.0 OF 35261302 35854529 (Patch for Bug 35854529).
- Patch 33421125: MEMORY LEAK IN 'KOLASLASSIGN' AND PGA INCREASES WHEN PGA LIMIT IS HIGHER (Part of DB RU19 Patch 35042068).
- Patch 35799058: SLOW EXPDP OF PARTITIONED TABLE EM_METRIC_VALUES_E (ENTERPRISE MANAGER REPOSITORY).

Timezone Prerequisite

The timezone of the source and target databases should be same.

For example, you can check the timezone in Linux by running: `timedatectl`

Tablespace Considerations

- **Tablespace creation:** Tablespaces need to be explicitly created using `SMALLFILE`. Preallocate the necessary data files.
- **Tablespace size:**

- Query the size of the tablespaces: MGMT_TABLESPACE, MGMT_ECM_DEPOT_TS and MGMT_AD4J_TS on the source database and recreate them on the target database.
- TEMP and UNDO tablespaces:
 - * Max UNDO space used seen during import is 680 MB.
 - * Max TEMP space used seen during import is 140 GB.

Note

For instructions about creating tablespaces manually, see [Step 2.2. Create Tablespaces in Target Database](#).

Other Recommendations

- **RAC environment:** Use connect string-based connection on the first node for RAC environment. Scan address is not supported.
- **Parallel environment:**
 - Export: Use no more than half the cores. The default value is 16.
 - Import: Use no more than the number of cores. The default value is 16.
 - Parallel jobs database parameters recommendations:
 - * For single instance: `max_datapump_parallel_per_job=200`
 - * For CDB/PDB: Set the following parameters in both databases:
 - * `max_datapump_jobs_per_pdb=200`
 - * `max_datapump_parallel_per_job=400`

Step 1.2. Complete Source Database Prerequisites

See below the prerequisites for the source database (ASM and non-ASM) when using RepMigrate utility for repository migration:

1. The source and target databases should be both at the same database release update (DB RU) version and with the same database patches installed.
Confirm all the database patches have been applied to the **source database** as described in [Step 1.1. Perform Common Prerequisites for Source and Target Databases](#).
2. For TDE only, ensure to pass the same RepMigrate `-encryptionPassword` parameter to the source and target databases. When running the RepMigrate export operation in the source database using the `-encryptionPassword` parameter, after you need to pass the same `-encryptionPassword` parameter value during the RepMigrate import operation in the target database. For RepMigrate information, see [RepMigrate Usage](#).
3. Before starting the repository migration process, confirm the **source host** has enough space available to store the files (dumpfiles) that will get created during the export operation.
 - Perform tablespace validation.
Check if the destination directory specified for the dumpfiles location can accommodate the contents of the database and confirm that there's enough space in the source host.

Step 1.3. Complete Target Database Prerequisites

See below the prerequisites for the target database when using RepMigrate utility for repository migration:

1. The source and target databases should be both at the same Database Release Update (DB RU) version and with the same database patches installed.
Confirm all the database patches have been applied to the **target database** as described in [Step 1.1. Perform Common Prerequisites for Source and Target Databases](#).
2. The *Management Agent* should be pushed to the **target database** and patched using the same Enterprise Manager Release Update (RU) version as the one used by the OMS before starting the repository migration.
For information about Enterprise Manager requirements, see [Step 1.4. Perform Common Prerequisites for Source and Target Enterprise Manager Hosts](#).
3. For SSL configured databases, use DB Wallet created at the source database using the EM Oracle Home to ensure same JDK version is used.
For TDE, ensure to pass the same RepMigrate `-encryptionPassword` parameter to the source and target databases. When running the RepMigrate import operation in the **target database**, you need to pass the same `-encryptionPassword` parameter value that was passed during the RepMigrate export operation in the source database. For RepMigrate information, see [RepMigrate Usage](#).
4. Before starting the repository migration process, confirm the **target host** has enough space available to store the files (dumpfiles) that will get used for the import operation.
 - Perform tablespace validation.
Check if the directory specified for the dumpfiles location for the import operation can accommodate the contents of the database and confirm that there's enough space in the target host.
5. To minimize downtime, get the target database ready before the repository migration process is performed. For details, see [Step 2. Best Practices](#).

Step 1.4. Perform Common Prerequisites for Source and Target Enterprise Manager Hosts

The following lists the common Enterprise Manager prerequisites when using RepMigrate utility for repository migration:

1. Apply the necessary Enterprise Manager Release Update (RU) version to both the *source* and *target OMS* environments.
The Enterprise Manager Release Update version should be the same on the *source* and *target OMS hosts* and the *RepMigrate* utility. For information about RepMigrate, see [How to Get RepMigrate Utility?](#).
2. Apply the necessary Enterprise Manager Release Update version to the centralized **Management Agents**.
The Enterprise Manager Management Agent on the source and target hosts must be at the same Enterprise Manager RU version.
3. Add the correct Enterprise Manager Release Update (RU) Agent to the **primary target database** node.

Step 2. Best Practices

Complete the following steps in the **target database** to minimize downtime:

- [Step 2.1. Check Database Objects](#)

- [Step 2.2. Create Tablespaces in Target Database](#)
- [Step 2.3. RAC only: Create RAC Services](#)

Step 2.1. Check Database Objects

To minimize the downtime, it's important to confirm that the **target database** is ready for the repository migration.

Oracle recommends to check the following in the target database before starting the repository migration process:

- Tablespaces already created.
- Tablespaces sized according to your requirements.
- Database parameters updated.
- Non-Enterprise Manager roles and users already created.
- Any external profiles to be kept should get created.
- Legacy users either dropped on the source database or created on the target database.
- DBA directories to be kept from the source database created on the target database.
- Storage checked.
- If using RAC services, jobs should be already created.

Step 2.2. Create Tablespaces in Target Database

To minimize downtime, it's important to perform this step in the **target database** before starting the repository migration.

Create tablespaces in the target database manually by doing the following:

1. Check the size of the tablespace in the source database for MGMT, ECM_DEPOT and AD4J tablespaces by using the below query as SYS user:

```
select sum(bytes)/1024/1024 SIZE_IN_MB from dba_segments
where tablespace_name='MGMT_TABLESPACE';
```

```
select sum(bytes)/1024/1024 SIZE_IN_MB from dba_segments
where tablespace_name='MGMT_ECM_DEPOT_TS';
```

```
select sum(bytes)/1024/1024 SIZE_IN_MB from dba_segments
where tablespace_name='MGMT_AD4J_TS';
```

2. Using above output as sizes, create tablespaces using below queries:

```
CREATE SMALLFILE TABLESPACE "MGMT_AD4J_TS" EXTENT MANAGEMENT LOCAL
AUTOALLOCATE SEGMENT SPACE MANAGEMENT AUTO
DATAFILE '<datafileLocation>/mgmt_ad4j.dbf' SIZE
<MGMT_AD4J_TS_size_as_calculated>
REUSE AUTOEXTEND ON NEXT 50M MAXSIZE UNLIMITED;
```

```
CREATE SMALLFILE TABLESPACE "MGMT_ECM_DEPOT_TS" EXTENT MANAGEMENT LOCAL
AUTOALLOCATE SEGMENT SPACE MANAGEMENT AUTO
DATAFILE '<datafileLocation>/mgmt_depot.dbf' SIZE
<MGMT_ECM_DEPOT_TS_size_as_calculated>
```

```
REUSE AUTOEXTEND ON NEXT 20M MAXSIZE UNLIMITED;  
  
CREATE SMALLFILE TABLESPACE "MGMT_TABLESPACE" EXTENT MANAGEMENT LOCAL  
AUTOALLOCATE SEGMENT SPACE MANAGEMENT AUTO  
DATAFILE '<datafileLocation>/mgmt.dbf' SIZE  
<MGMT_TABLESPACE_size_as_calculated>  
REUSE AUTOEXTEND ON NEXT 50M MAXSIZE UNLIMITED;
```

Note

The value of the <datafileLocation> should be similar to what you used in source database host.

- For TEMP and UNDO tablespaces, Oracle recommends to have size around the following:
 - Max PDB Temp Usage = 140 GB
 - Max PDB Undo Usage = 680 MB

RepMigrate utility checks for TEMP and UNDO tablespaces. If there's not enough space available, it will fail.

Step 2.3. RAC only: Create RAC Services

To minimize downtime, it's important to perform this step in the **target database** before starting the repository migration.

This is only applicable to RAC environments: If RAC services are used in the source database, you must create the required RAC services in the target database.

For information about sizing, see [Software Configurations](#) in the *Enterprise Manager Advanced Installation and Configuration Guide*.

For information about RAC service links creation, see [Jobs](#) in the *Enterprise Manager Advanced Installation and Configuration Guide*.

Step 3. Run Prerequisites Check

Complete the following steps in the source database to run the *RepMigrate* utility and check only the prerequisites prior to starting the repository migration (export operation) and proactively resolve any issues.

Note

Before proceeding, confirm that the database prerequisites have been completed. For details, see [Step 1.1. Perform Common Prerequisites for Source and Target Databases](#).

- Run RepMigrate to only check the prerequisites in the **source database** using the `-prereqOnly` parameter.

For example:

```
./RepMigrate.sh -prereqOnly -dbUser sys -dbPassword <db password> -  
connectString "<connect string>" -dataPumpDir <data pump dir location> -
```

```
datapumpUser <datapump user> -datapumpPassword <datapump password> -action  
expdp -dbHome <db home location> -reposPassword <repos Password> [-  
parallel <number>]
```

2. Address any issues reported from the standard output.

Repeat step 1 until you are satisfied and correct all you need.

When using the `-prereqOnly` parameter, you can check for issues with external users, external profiles, external roles, external directories, legacy EM schemas, such as `SYSMAN_BIPLATFORM` and `SYSMAN_APM`, DBMS scheduler jobs and invalid objects in external schemas. After receiving the report, follow the instructions as shown by RepMigrate to resolve any issues. Then, execute the RepMigrate again (step 1). If there are still issues, you can decide to ignore them by using the `-ignorePrereqList` parameter. If you pass the `-ignorePrereqList` without following the instructions, the import operation will result into failures.

Note

For RAC environment, use the connect string-based connection on the first node for the RAC setup. Scan address is not supported.

For SSL configured repository, use `RepMigrate.sh -help` to review the available options.

For more information about RepMigrate utility, see [RepMigrate Usage](#).

Step 4. Perform Migration

After completing the previous steps, perform the following to migrate the repository database using RepMigrate:

- [Step 4.1. Shutdown OMS and Agent](#)
- [Step 4.2. Restart Source Database](#)
- [Step 4.3. Export from Source Database Using RepMigrate](#)
- [Step 4.4. Copy Dumpfiles from Source to Target](#)
- [Step 4.5. Import into Target Database Using RepMigrate](#)
- [Step 4.6. Set Up New Repository](#)

Step 4.1. Shutdown OMS and Agent

To shutdown Enterprise Manager OMS and Management Agents, connect to the **source host** and do the following:

1. Stop the OMS from the `$OMS_Home/bin` directory.

```
emctl stop oms -all -force
```

Note

If there are multiple OMS environments then stop each OMS and agent on all nodes.

2. Stop the Management Agent.

```
emctl stop agent
```

3. Stop all central Management Agents.

4. Purge recyclebin as SYSMAN user.

Connect to the source repository database as SYSMAN user and execute the following:

```
SQL> PURGE RECYCLEBIN;
```

Step 4.2. Restart Source Database

Shutdown and restart the **source databases** including pluggable databases.

- If the OMS Repository is in a single instance database, then the database needs to be shutdown and restart.
- If the OMS Repository is in a pluggable database, then only the pluggable database needs to be shutdown and restart.
- If the OMS Repository is in a RAC environment, then shutdown and restart all database instances.

Step 4.3. Export from Source Database Using RepMigrate

You can now proceed with the export operation from the **source database** using the RepMigrate utility.

See below the steps that need to be executed in the source database for a successful export operation in cross platform cross endian Repository Database:

- Invoke RepMigrate in command line.

```
./RepMigrate.sh -dbUser sys -dbPassword <db password> -connectString  
"<connect string>" -dataPumpDir <data pump dir location> -dataPumpUser  
<datapump user> -dataPumpPassword <datapump password> -action expdp -  
dbHome <db home location> -reposPassword <repos Password> [-parallel  
<number>]
```

Where:

- <db password> is the password of SYS database user.
- <connect string> is the Enterprise Manager Repository database connect string.
- <data pump dir location> is the destination location where the datapump export dump files will be copied to.
- <datapump user> is SYSTEM database user or user with EXP_FULL_DATABASE privilege.
- <datapump password> is the password of the datapump user. In this case, the SYSTEM user password.
- <db home location> is the database home of the Enterprise Manager Repository.
- <repos Password> is the password of SYSMAN database user.
- -parallel <number> is optional. It's the number of parallel workers. Default is 16.

Note

For ASM environment, you need to pass the ASM specific location for the `-dataPumpDir <data pumpdir location>` parameter. For example:

```
-dataPumpDir +DATAC1/DP_EXPORT_DIR
```

For information about RepMigrate utility, see [RepMigrate Usage](#).

Example

```
./RepMigrate.sh -dbUser sys -dbPassword abc -connectString
"(DESCRIPTION=(ADDRESS=(PROTOCOL=abc)(HOST=abchostname)(PORT=0000))
(CONNECT_DATA=(SERVER=DEDICATED)(SID=sidname)))" -dataPumpDir /abc/dirname -
dataPumpUser system -dataPumpPassword abc -action expdp -dbHome /abc/db_home -
reposPassword abc
```

Alternatively, you can invoke RepMigrate using a response file. For details, see [RepMigrate Response Files](#).

Output

Output looks similar to the following:

```
Looking for suitable Agent.
_agentRUVersion=13.5.0.22
Arguments validated Successfully
RepMigrate invoked with command line parameters: -action expdp -
dataPumpPassword ***** -dataPumpUser system -dataPumpDir /abc/dirname -
dbUser sys-dbPassword ***** -reposPassword ***** -script_dir /abc/
RepMigrate -connectString (DESCRIPTION=(ADDRESS=(PROTOCOL=abc)
(HOST=abchostname)(PORT=0000))(CONNECT_DATA=(SERVER=DEDICATED)(SID=sidname)))
-dbHome /abc/db_home
RepMigrate parameters from command line: -action expdp -dataPumpPassword
***** -dataPumpUser system -dataPumpDir /abc/dirname -dbUser sys -
dbPassword ***** -reposPassword ***** -script_dir /abc/RepMigrate -
connectString (DESCRIPTION=(ADDRESS=(PROTOCOL=abc)(HOST=abchostname)
(PORT=0000))(CONNECT_DATA=(SERVER=DEDICATED)(SID=sidname))) -dbHome /abc/
db_home
DB Patch 30978304applied.
External Role check passed.
External User check passed.
External Profile check passed.
Legacy User check passed.
DBMS Scheduler Jobs check passed.
Invalid Objects check passed.
DBA Directory check passed.
Directory Created Successfully
Directory Created Successfully
Stopping AQ...
RCU Logfile: /abc/RepMigrate/logs/rcu.log
Processing command line ....
Repository Creation Utility - Checking Prerequisites
Checking Global Prerequisites
```

```

Repository Creation Utility - Checking Prerequisites
Checking Component Prerequisites
Repository Creation Utility - Creating Tablespaces
Validating and Creating Tablespaces
Create tablespaces in the repository database
Repository Creation Utility - Create
Repository Create in progress.
Executing pre create operations
    Percent Complete: 55
    ...
Creating DB Migration Utility(EM_REPOS_MIGRATE_EXPORT)
    Percent Complete: 84
Executing post create operations
    Percent Complete: 100

Repository Creation Utility: Create - Completion Summary

Database details:
-----
Connect Descriptor                               :
(DESCRIPTION=(ADDRESS=(PROTOCOL=abc) (HOST=abchostname) (PORT=0000))
(CONNECT_DATA=(SERVER=DEDICATED) (SID=sidname)))
Connected As                                     : SYS
RCU Logfile                                       : /abc/RepMigrate/logs/rcu.log

Component schemas created:
-----
Component                                     Status      Logfile

DB Migration Utility                         Success     /abc/RepMigrate/
logs/em_repos_migrate_export.log

Repository Creation Utility - Create : Operation Completed
Please copy the logs folder from baseHome to a safe location if you plan to
delete the baseHome folder where baseHome is the location where the
RepMigrate Utility is unzipped.

```

Log Files

Check the log files in the <full_path_RepMigrate_location>/logs directory. For more details, see [RepMigrate Log Files](#).

Step 4.4. Copy Dumpfiles from Source to Target

Once the export operation is completed, copy the contents from the -dataPumpDir location used during the export operation from the source to the target host.

- Copy everything under -dataPumpDir location from source to target.
- Copy `admin_gen_grants_to_ro_user.sql` and `carry_info.txt` files from \$BASE_DIR where BASE_DIR value is where you unzipped the RepMigrate utility on the source host to the target host under \$BASE_DIR where you unzipped the RepMigrate utility.
- For ASM, do the following:

- Copy from the ASM source host to the ASM target host using the following:

```
asmcmd cp +DATA1/DP_MIGRATE_DIR/* sys/<pwd>@<IPAddress>.+ASM1:+DATA1/DP_MIGRATE_DIR
```

Where <pwd> is the ASM SYS password.

Step 4.5. Import into Target Database Using RepMigrate

You can now proceed with the import operation into the **target database** using the RepMigrate utility.

See below the steps that need to be executed in the target database for a successful import operation in cross platform cross endian Repository Database:

Invoke RepMigrate in command line.

```
./RepMigrate.sh -dbUser sys -dbPassword <db password> -connectString
"<connect string>" -dataPumpDir <data pump dir location> -dataPumpUser
<datapump user> -dataPumpPassword <datapump password> -action impdp -dbHome
<db home location> -reposPassword <repos Password> [-datafileLocation
<Location To Create Datafiles>] [-parallel <number>]
```

Where:

- <db password> is the password of SYS database user.
- <connect string> is the Enterprise Manager Repository database connect string.
- <data pump dir location> is the destination location where the datapump export dump files will be copied to.
- <datapump user> is SYSTEM database user or user with IMP_FULL_DATABASE privilege.
- <datapump password> is the password of the datapump user. In this case, the SYSTEM user password.
- <db home location> is the database home of the Enterprise Manager Repository.
- <repos Password> is the password of SYSMAN database user.
The -reposPassword <repos Password> value must be the same as the one used for the source database.
- -datafileLocation <Location To Create Datafiles>] is optional. It's the location to create the datafiles.
- -parallel <number> is optional. It's the number of parallel workers. Default value is 16.

① Note

- The RepMigrate utility sets job queue process and submits jobs on target by default. You can stop this by adding -keepQuiesce.
- For ASM, provide an extra parameter: -datafileLocation <Location to Datafile>.

Example

```
./RepMigrate.sh -dbUser sys -dbPassword abc -connectString
(DESCRIPTION=(ADDRESS=(PROTOCOL=abc)(HOST=123hostname)(PORT=0000))
(CONNECT_DATA=(SERVER=DEDICATED)(SID=sidname))) -dataPumpDir /abc/dirname -
dataPumpUser system -dataPumpPassword abc -action impdp -dbHome /abc/db_home -
reposPassword abc
```

Alternatively, you can invoke RepMigrate using a response files. For details, see [RepMigrate Response Files](#).

Output

Output looks similar to the following:

```
Looking for suitable Agent.
_agentRUVersion=13.5.0.22
Arguments validated Successfully
RepMigrate invoked with command line parameters: -action impdp -
dataPumpPassword ***** -dataPumpUser system -dataPumpDir /abc/dirname -
dbUser sys -dbPassword ***** -reposPassword ***** -connectString
(DESCRIPTION=(ADDRESS=(PROTOCOL=abc)(HOST=abchostname)(PORT=0000))
(CONNECT_DATA=(SERVER=DEDICATED)(SID=sidname))) -dbHome /abc/db_home
RepMigrate parameters from command line: -action impdp -dataPumpPassword
***** -dataPumpUser system -dataPumpDir /abc/dirname -dbUser sys -
dbPassword ***** -reposPassword ***** -connectString
(DESCRIPTION=(ADDRESS=(PROTOCOL=abc)(HOST=abchostname)(PORT=0000))
(CONNECT_DATA=(SERVER=DEDICATED)(SID=sidname))) -dbHome /abc/db_home
DB Patch 30978304 applied.
Directory Created Successfully
Datafile Folder Validated
Directory Created Successfully
Folder already exists. Skipping creation of the folder.
    RCU Logfile: /abc/RepMigrate/logs/rcu.log
Processing command line ....
Repository Creation Utility - Checking Prerequisites
Checking Global Prerequisites
Repository Creation Utility - Checking Prerequisites
Checking Component Prerequisites
Repository Creation Utility - Creating Tablespaces
Validating and Creating Tablespaces
Create tablespaces in the repository database
Repository Creation Utility - Create
Repository Create in progress.
Executing pre create
    operations
    Percent Complete: 55
    ...
Creating DB Migration Utility(EM_REPOS_MIGRATE_IMPORT)
    Percent Complete: 84
Executing post create operations
    Percent Complete: 100

Repository Creation Utility: Create - Completion Summary

Database details:
```

```

-----
Connect Descriptor                               :
(DESCRIPTION=(ADDRESS=(PROTOCOL=TCP)(HOST=em1111.subnetaaa.bbbb.oraclevcn.com)
(PORT=1521))(CONNECT_DATA=(SERVER=DEDICATED)(SID=orcl)))
Connected As                                     : SYS
RCU Logfile                                     : /abc/RepMigrate/logs/rcu.log

```

Component schemas created:

```

-----
Component                                     Status      Logfile
DB Migration Utility                         Success     /abc/RepMigrate/
logs/em_repos_migrate_import.log

```

Repository Creation Utility - Create : Operation Completed
Please copy the logs folder from baseHome to a safe location if you plan to delete the baseHome folder where baseHome is the location where the RepMigrate Utility is unzipped.
Starting AQ.

Log File

Check the log files in the <full_path_RepMigrate_location>/logs directory. For more details, see [RepMigrate Log Files](#).

Step 4.6. Set Up New Repository

To set up the new repository, do the following:

- Restart Enterprise Manager OMS with admin option.
 - emctl start oms -admin_only
- Change OMS configuration.

```

emctl config oms -store_repos_details -repos_conn_desc
'(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<Host_NAME>)
(PORT=<Port>)))(CONNECT_DATA=(SERVER=DEDICATED)(SERVICE_NAME=<Service>)))'
-repos_user SYSMAN -repos_pwd <pwd>

```

```

emctl config emrep -sysman_pwd <sysman password> -conn_desc "new DB
descriptor"

```

- Change all services used by Enterprise Manager.
For RAC, Enterprise Manager has a connect string for certain subsystems that use RAC services. If those are configured, they need to be changed. For information, see the *Enterprise Manager Advanced Installation and Configuration Guide*.
- Stop OMS.
 - emctl stop oms -all
- Restart OMS and Management Agent.
 - emctl start oms
 - emctl start agent

Perform Post Migration Verification

These verification steps should be carried out post migration to ensure that the migration was completely successful:

- Verify any discrepancy in objects by comparing source and target databases through Enterprise Manager.
- Verify the migrated database through Enterprise Manager to determine whether the database is running without any issues.
- Verify the repository operations, dbms jobs and whether any management system errors are reported.
- Verify that all Enterprise Manager functionalities are working correctly after the migration.
- Make sure Management Services and the Repository target is properly relocated by verifying it through Enterprise Manager.

RepMigrate Files and Troubleshooting

Starting with Enterprise Manager 13c Release 5 Update 22 (13.5.0.22), the RepMigrate utility is available for performing Enterprise Manager repository database migration.

This section provides additional information about the RepMigrate utility such as log and response files, and troubleshooting.

- [RepMigrate Log Files](#)
- [RepMigrate Response Files](#)
- [Troubleshoot RepMigrate](#)

RepMigrate Log Files

This section provides information about the log files generated when using the RepMigrate utility.

Location

They are located in the <RepMigrate_location>/logs folder.

- [Export Log Files](#)
- [Import Log Files](#)

Export Log Files

The following are the contents of the RepMigrate export log files:

- em_repos_migrate_export.log
- error.txt
- export/
 - restOfSchemasExportOutput.log
 - sysmanTypesDataOnlySchemaExportOutput.log
 - sysmanUsersOnlyExportOutput.log
 - tableExportOutput.log

- viewExportOutput.log
- logger<number>.properties where <number> is a random number generated.
- output.txt
- rcu.log
- repmigrate/
 - m_<timestamp>.expdp where <timestamp> is date and time generated.
 - * repmigrate_expdp.log

Import Log Files

The following are the contents of the RepMigrate import log files:

- custom_comp_create_tbs.log
- import/
 - restOfSchemasImportOutput.log
 - sysmanTypesDataOnlySchemaImportOutput.log
 - sysmanUsersOnlyImportOutput.log
 - tableImportOutput.log
 - viewImportOutput.log
- output.txt
- repmigrate/
 - m_<timestamp>.impdp where <timestamp> is date and time generated.
 - * repmigrate_impdp.log
- em_repos_migrate_import.log
- error.txt
- logger<number>.properties where <number> is a random number generated.
- rcu.log
- utlprp.sql

RepMigrate Response Files

This section provides information about invoking RepMigrate using response files.

You can create response files and use them when invoking RepMigrate utility.

Response Files Location

They can be created and saved under the RepMigrate home directory (location where RepMigrate was unzipped).

- [Export Response File](#)
- [Import Response File](#)
- [Invoke Response File Using RepMigrate](#)

Export Response File

You can create a response file using a text editor, add the required parameters for the export operation and save it with any preferred name. For example, it can be saved as `<RepMigrate_location>/repmigrate_exp.rsp` file.

Response File Example for Export:

```
action=expdp
connectString=(DESCRIPTION=(ADDRESS=(PROTOCOL=abc)(HOST=abchohostname)
(PORT=0000))(CONNECT_DATA=(SERVER=DEDICATED)(SID=sidname)))
dbUser=SYS
dbPassword=welcome***
reposPassword=welcome***
dataPumpUser=SYSTEM
dataPumpPassword=welcome***
dataPumpDir=/abc/dirname
dbHome=/abc/db_home
```

For information about the above parameters and values, see [Step 4.3. Export from Source Database Using RepMigrate](#).

Import Response File

You can create a response file using a text editor, add the required parameters for the import operation and save it with any preferred name. For example, it can be saved as `<RepMigrate_location>/repmigrate_imp.rsp` file.

Response File Example for Import:

```
action=impdp
connectString=(DESCRIPTION=(ADDRESS=(PROTOCOL=abc)(HOST=abchohostname)
(PORT=0000))(CONNECT_DATA=(SERVER=DEDICATED)(SID=sidname)))
dbUser=SYS
dbPassword=welcome****
reposPassword=welcome***
dataPumpUser=SYSTEM
dataPumpPassword=welcome***
dataPumpDir=/abc/dirname
dbHome /abc/em/db_home
```

For information about the above parameters and values, see [Step 4.5. Import into Target Database Using RepMigrate](#).

Invoke RepMigrate Using Response File

To invoke RepMigrate using a response file, run the following:

```
RepMigrate.sh -responsefile <full_path_response_file>
```

Export example:

```
RepMigrate.sh -responsefile /abc/repmigrate_exp.rsp
```

Troubleshoot RepMigrate

This section covers some typical issues and resolutions related to the *RepMigrate* utility.

Users may encounter various errors during the repository migration process. Causes and recommended actions for some common errors are listed below.

- [Agent home does not have the same RU version as that of OMS. Ensure that the agent is patched with the same RU version as the OMS and then retry the operation.](#)
- [DB Patch 30978304 is not found. Please contact Oracle Support to resolve this error.](#)
- [External User check failed. Create EM_ADMIN user on target DB before import.](#)
- [External Role check failed. Create SYSMAN_READ1 role on target DB before import.](#)
- [External Profiles check failed. Create PGGD profile on target DB before import.](#)
- [Recovery of Old Enterprise Manager](#)
- [Recovery from Failure during Export](#)
- [Recovery from Failure during Import](#)

Agent home does not have the same RU version as that of OMS. Ensure that the agent is patched with the same RU version as the OMS and then retry the operation.

Cause: *RepMigrate* utility requires EM agent with the same release update (RU) level of the OMS to be running on the source and target database host. Utility provides the above error if the EM agent is not running on the source or target host.

Action: Push an EM agent with same RU as the OMS to the source or target host before performing the export (expdp) or import (impdp) operation.

DB Patch 30978304 is not found. Please contact Oracle Support to resolve this error.

Cause: *RepMigrate* utility requires Data Pump patch 30978304 to be applied on both source and target hosts before the expdp or impdp operation. Utility throws this error if the patch is not applied on source or target host.

Possible Action: Contact [My Oracle Support](#) and apply the database patch 30978304 or the Data Pump patch specific to the database version on the source or target host. For database patch information, see [My Oracle Support](#).

External User check failed. Create EM_ADMIN user on target DB before import.

Cause: *RepMigrate* utility checks for any external users other than EM users created on the source database. If it finds external users, it throws this error with all the names of external users in the source. In the above example, EM_ADMIN is an external user.

Possible Action: User must create the external users listed in the error on the target.

User should rerun the utility by passing `-ignorePrereqList` `repmigrate_external_user_check` parameter.

The same information would be displayed on the console along with the error as below:

Re-run the RepMigrate utility on the source database with the "-ignorePrereqList repmigrate_external_user_check" option to complete the export operation. If more than one prereq has failed pass them with comma (,) separated list. For example: "-ignorePrereqList repmigrate_<x>_check,repmigrate_<y>_check". Use RepMigrate -help on usage.

External Role check failed. Create SYSMAN_READ1 role on target DB before import.

Cause: *RepMigrate* utility checks for any external roles other than EM roles created on the source database. If it finds external roles, it throws this error with all the names of external roles in the source. In the above example, SYSMAN_READ1 is an external role.

Possible Action: User must create the external roles listed in the error on the target.

User should rerun the utility by passing `-ignorePrereqList repmigrate_external_roles_check` parameter.

The same information would be displayed on the console along with the error as below:

Re-run the RepMigrate utility on the source database with the "-ignorePrereqList repmigrate_external_role_check" option to complete the export operation. If more than one prereq has failed pass them with comma (,) separated list e.g. "-ignorePrereqList repmigrate_<x>_check,repmigrate_<y>_check". Use RepMigrate -help on usage.

External Profiles check failed. Create PGGD profile on target DB before import.

Cause: *RepMigrate* utility checks for any external profiles other than EM profiles created on the source DB . If it finds external profiles, it throws this error with all the names of external profiles in the source. In this example, PGDB is an external profile.

Possible Action: User must create the external profiles listed in the error on the target.

User should rerun the utility by passing `-ignorePrereqList repmigrate_external_profile_check` parameter.

The same information would be displayed on the console along with the error as below:

Re-run the RepMigrate utility on the source database with the "-ignorePrereqList repmigrate_external_profile_check" option to complete the export operation. If more than one prereq has failed pass them with comma (,) separated list e.g. "-ignorePrereqList repmigrate_<x>_check,repmigrate_<y>_check". Use RepMigrate -help on usage.

Recovery of Old Enterprise Manager

To recover old EM, run the below as SYS on source database:

1. ALTER SYSTEM SET job_queue_processes=<JOB_QUEUE_MAX> sid='*'; where JOB_QUEUE_MAX can be checked from carry_info.txt file present in <dataPumpDir>.

For ASM, the value of JOB_QUEUE_MAX can be checked from carry_info.txt file located in <BASEDIR>.

2. ALTER SESSION SET CURRENT_SCHEMA = SYSMAN;
3. @<baseDir>/rsc/sql/admin_submit_dbms_jobs.sql;

The <baseDir> is the location where *RepMigrate* is unzipped.

4. Run below as SYSMAN to start AQ:

```
begin
for emqrec in (select name from dba_queues where owner='SYSMAN' and name
```

```

not like 'AQ$%')
loop
DBMS_AQADM.start_queue(
    queue_name => emqrec.name,
    enqueue =>    true,
    dequeue => true);
end loop;
end;

/

```

5. Start OMS

```
emctl start oms
```

6. Start Agent

```
emctl start agent
```

Recovery from Failure during Export

In case of failure during Export, do the following:

1. Run following on source database as SYS:

```

ALTER SYSTEM SET job_queue_processes=<JOB_QUEUE_MAX> sid='*'; where
JOB_QUEUE_MAX can be checked from carry_info.txt file present in
<dataPumpDir>.

```

For ASM, the value of JOB_QUEUE_MAX can be checked from carry_info.txt file present in <baseDir>.

```
ALTER SESSION SET CURRENT_SCHEMA = SYSMAN;
```

```
@<baseDir>/rsc/sql/admin_submit_dbms_jobs.sql;
```

The <baseDir> is the location where *RepMigrate* is unzipped.

2. Run below as SYSMAN to start AQ:

```

begin
for emqrec in (select name from dba_queues where owner='SYSMAN' and name
not like 'AQ$%')
loop
DBMS_AQADM.start_queue(
    queue_name => emqrec.name,
    enqueue =>    true,
    dequeue => true);
end loop;
end;

/

```

3. Delete the following:

- The <dumpfile folder> passed to utility in step 3 as provided in -dataPumpDir option.

- <baseDir/logs> folder.
- For ASM, in addition to above steps, delete the `carry_info.txt` and `admin_gen_grants_to_ro_user.sql` from <baseDir>.
- Retry Export.

Recovery from Failure during Import

1. Remove the old DB instance.
If the old database instance is a CDB and you are importing to a PDB, you can delete and recreate the PDB.
2. Create a new instance.
3. Delete <baseDir/logs> folder in <baseDir> before retrying the import.
The <baseDir> is the location where *RepMigrate* is unzipped.
4. For ASM, in addition to above steps, delete the DUMPSET using ASMCMD by doing the following:
 - Login to ASMCMD.
 - Got to the DUMPSET of the ASM Instance.
 - Run the following:

```
rm sysman_*  
rm view.dmp  
rm table.dmp
```

3

Configuring a Software Library

This chapter describes how you can configure a new Software Library using Enterprise Manager console, the various users and the privileges required to access the Software Library, and finally how to maintain an existing Software Library in the Enterprise Manager environment.

Note

Oracle strongly recommends that you select the **Configure Oracle Software Library** option and configure it at the time of installation so that the installer can automatically configure it for you, thus saving your time and effort. For more information on this, see *Oracle Enterprise Manager Basic Installation Guide*.

However, if you have not already configured the Software Library, you can do so from the Enterprise Manager console as described in this chapter.

In particular, this chapter covers the following:

- [Overview of Software Library](#)
- [Users, Roles, and Privileges](#)
- [Performing Software Library Tasks Using EM CLI Verbs or in Graphical Mode](#)
- [Software Library Storage](#)
- [Prerequisites for Configuring Software Library](#)
- [Configuring Software Library Storage Location](#)
- [Configuring Software Library on a Multi-OMS System](#)
- [Software Library Cache Nodes](#)
- [Software Library File Transfers](#)
- [Using Software Library Entities](#)
- [Tasks Performed Using the Software Library Home Page](#)
- [Maintaining Software Library](#)

Overview of Software Library

Oracle Software Library (Software Library) is one of the core features offered by Enterprise Manager. Technically, it is a repository that stores 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, from the **Enterprise** menu, select **Jobs and Procedures**, then click **Software Library**. On the Software Library home page, as shown in

[Figure 3-1](#), there are two types of folders: Oracle-owned folders (marked by a lock symbol) and User-owned folders.

Oracle-owned folders and their contents (including other subfolders and entities) offered with the product by default, and appear on the Software Library home page after Software Library is configured. User-owned folders are logical top level folders that the user creates to organize the entities that he/she intends to create.

Figure 3-1 Software Library Console

The screenshot shows the 'Software Library: Administration' page. It includes a breadcrumb 'Software Library > Software Library: Administration' and a status bar 'Page Refreshed Nov 18, 2015 11:24:19 AM UTC'. The main content area has tabs for 'Upload File Locations', 'Referenced File Locations', and 'Cache Nodes'. Below the tabs, there's a section for 'Storage Type' set to 'OMS Shared File System'. A table lists storage locations with columns: Name, Status, Location, Associated Entities, Credential, Total Space, Available Space, Used Space, Deleted Entities Used Space, and Last Refreshed. One entry is visible with Name 'swlib', Status 'Active', Location '/net/sc042b/scratch/csadmin/swlib/', and various space metrics.

Name	Status	Location	Associated Entities	Credential	Total Space	Available Space	Used Space	Deleted Entities Used Space	Last Refreshed
swlib	Active	/net/sc042b/scratch/csadmin/swlib/	Show	Change Credential Clear credential	232.69 GB	153.58 GB	16.61 GB	0 Bytes	Nov 18, 2015 11:03:24 AM UTC

The Software Library Page facilitates storage of Enterprise Manager entities. For example,

- Self Update entities like plug-ins, connectors, DB workload, and so on.
- Provisioning and Patching entities like gold images, application archives, Perl/shell scripts, and so on.

Advantages:

- Software Library supports patching and provisioning in Online mode and Offline mode. For example, if database patches cannot be downloaded directly from *My Oracle Support*, you can download them separately, and stage them from Software Library for offline deployment.
- The Software Library allows you to leverage your organizations existing IT infrastructure (like file servers, web servers, or storage systems) to stage the files to host targets as part of a provisioning or patching activity using Referenced File Locations.
- Software Library allows you to organize the entities, which basically refer to the software binaries or directive scripts in your enterprise, into logical folders for efficient management.

From the Software Library Console page, you can perform the following tasks:

- Configure Software Library Storage, see [Configuring Software Library Storage Location](#) for more information.
- Create Software Library Entities. For example, Creating a Generic Component, Creating Directives, and so on.
- Manage Software Library Entities. For example, Viewing Entities, Editing Entities, Deleting Entities, Searching Entities, and so on.

Users, Roles, and Privileges

By default, all the Software Library folders and entities that are offered with the product are viewable by all the Enterprise Manager users. Fine grained privileges provide a way to control user access to the different entities in the Software Library. Administrators by default do not have any Software Library privileges, it is for the Super Administrator to grant access, privileges to an Administrator.

Note

To run any 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.

Software Library user roles can be broadly classified as:

- **Designers** are administrators who perform design time tasks such as setting up Software library, migrating entities, granting privileges to the Operators, deleting entities, and so on. They can perform both design time activities and run-time activities that the Operator can perform. Designers in Enterprise Manager can be granted Super Administrator role or the `EM_PROVISIONING_DESIGNER` role which allows him to create and maintain any Software Library entity.
- **Operators** are administrators who can perform run-time activities like deleting entities, changing the maturity status, and so on. Operators are typically granted roles like `EM_PROVISIONING_OPERATOR` or `EM_PATCH_OPERATOR` and so on.

Any Enterprise Manager user requires, at the very least, a view privilege on an entity for the entity to be visible on the Software Library Home page. Users will not be able to see this entity until the Super Administrator or the owner of the entity grants them at least a view privileges on the entity.

Note

All the folders and entities that are offered along with the product also known as the Oracle-owned entities, by default are viewable by all the Enterprise Manager users.

Administrator by default do not have any Software Library privileges, it is for the Super Administrator, to grant access, privileges to an Administrator. [Table 3-1](#) describes all the available Software Library privileges that can be granted to a user or role.

Users and roles can be granted privileges on specific entities by the owner of the entity or the Super Administrator. For more details, see *Oracle Enterprise Manager Administrator's Guide for Software and Server Provisioning and Patching*.

Table 3-1 Software Library Privileges for Administrators

Resource Type	Description
View any Template Entity	Ability to view any Template Entity
Export Any Software Library Entity	Ability to export any Software entity
Edit any Software Library Entity	Ability to edit any Software Library entity

Table 3-1 (Cont.) Software Library Privileges for Administrators

Resource Type	Description
Manage Any Software Library Entity	Ability to create, view, edit, and delete any Software Library entity
Import Any Software Library Entity	Ability to import any Software Library entity
Create Any Software Library Entity	Ability to create any Software Library entity
View Any Software Library Entity	Ability to view any Software Library entity
View Any Assembly Entity	Ability to view any Assembly entity
Grant Any Entity Privilege	Ability to grant view, edit, and delete privileges on any Software Library entity. This privilege is required if the user granting the privilege on any entity is not a Super Administrator or owner of the entity.

[Table 3-2](#) describes all the primary users of Software Library, and their associated privileges:

Table 3-2 Roles and Privileges

Role	Software Library Privileges
Super Administrator	All Software Library Privileges
EM_PROVISIONING_DESIGNER (Designer)	Create Any Software Library Entity
EM_PROVISIONING_OPERATOR (Operator)	View Any Software Library Entity
EM_PATCH_OPERATOR	Create Any Software Library Entity View Any Software Library Entity
EM_USER (Administrator)	Access Enterprise Manager

Super Administrators have complete privileges on all the entities present in Software Library, and can exercise access control on the entities by granting one or more privileges, and later revoking the previously granted privilege to another user or role.

Designers by default are given create privileges, which allow them to create entities and manage them.

Operators by default are given view privileges, which allow them to view all the entities in Enterprise Manager.

Any Enterprise Manager user requires, at the very least, a view privilege on an entity for the entity to be visible on the Software Library console. The Super Administrator can choose to grant additional privileges described in [Table 3-1](#) to the user or role. Users will not be able to see this entity till the Super Administrator grants them at least a view privilege on the entity.

Performing Software Library Tasks Using EM CLI Verbs or in Graphical Mode

You can perform some of the console-based Software Library operations using the command line utility and its Software Library verbs.

The following table describes both approaches to perform some of the Software Library tasks:

- Enterprise Manager Command Line Interface (EM CLI)
- Enterprise Manager Graphical User Interface (EM GUI)

Note

For more information about the syntax and usage of the EM CLI verbs described in [Table 3-3](#), along with workflow examples, refer to the *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

Table 3-3 Software Library EMCLI Verbs

Description	Approach A: Using EM CLI Verb	Approach B: Using Enterprise Manager Console
Adding a Software Library storage location	<code>add_swlib_storage_location</code>	Configuring an OMS Shared File system Location Configuring an OMS Agent File system Location Configuring a Referenced File Location
Creating a Software Library entity	<code>create_swlib_entity</code>	Creating Generic Components Creating Directives
Creating a Software Library folder	<code>create_swlib_folder</code>	Organizing Entities
Listing the Software Library entities	<code>list_swlib_entities</code>	Accessing Software Library Home Page Searching Entities
Listing Software Library entity types	<code>list_swlib_entity_types</code>	NA
Listing Software Library entity subtypes	<code>list_swlib_entity_subtypes</code>	NA
Listing Software Library folders	<code>list_swlib_folders</code>	NA
Listing Software Library storage locations	<code>list_swlib_storage_locations</code>	Accessing Software Library Administration Page
Referring files from a Software Library entity	<code>refer_swlib_entity_files</code>	Creating Entities Viewing, Editing, and Deleting Entities
Re-Importing Software Library metadata	<code>reimport_swlib_metadata</code>	Re-Importing Oracle Owned Entity Files
Removing a Software Library storage location	<code>remove_swlib_storage_location</code>	Removing (and Migrating) Software Library Storage Location
Modifying a Software Library entity	<code>update_swlib_entity</code>	Viewing, Editing, and Deleting Entities
Uploading files to a Software Library entity	<code>upload_swlib_entity_files</code>	Creating Entities Viewing, Editing, and Deleting Entities

Table 3-3 (Cont.) Software Library EMCLI Verbs

Description	Approach A: Using EM CLI Verb	Approach B: Using Enterprise Manager Console
Modifying a Software Library OMS Agent storage location to change the associated OMS Host and the credential for accessing the location.	<code>switch_swlib_oms_agent_storage</code>	NA
Verifying the files uploaded to software library, and reporting the missing files in the storage locations. This action is typically initiated when some provisioning/patching/deployment activity fails due to missing file in the associated storage location.	<code>verify_swlib</code>	NA
Staging one or more files associated with an entity revision available in the Software Library to a file system location on a host target.	<code>stage_swlib_entity_files</code>	Staging Entities
Staging one or more files associated with an entity revision in the Software Library to the local file system of a host not monitored by an EM Agent.	<code>stage_swlib_entity_files_local</code>	Staging Entities
Creating an entity of the Directive type in the Software Library. On successful creation, the entity revision appears in the specified folder on the Software Library Home page.	<code>create_swlib_directive_entity</code>	Creating Directives

Table 3-3 (Cont.) Software Library EMCLI Verbs

Description	Approach A: Using EM CLI Verb	Approach B: Using Enterprise Manager Console
Modifying an entity of the Directive type in the Software Library. A new revision of the entity is created by default. Changing only the description or attribute values do not create a new revision, and such changes are visible across all existing revisions of the entity	<code>update_swlib_directive_entity</code>	Viewing, Editing, and Deleting Entities
Listing all the details of an entity revision.	<code>get_swlib_entity_details</code>	Viewing, Editing, and Deleting Entities
Exporting files of Software Library entities to be imported on a cache node as cached files.	<code>export_swlib_cache_files</code>	Exporting and Importing Files for Cache Nodes
Importing Software Library entity files from a compressed file to a cache node.	<code>import_swlib_cache_files</code>	Exporting and Importing Files for Cache Nodes
Invoking resynchronize for one or all cache nodes.	<code>resync_swlib_cache</code>	Synchronizing the Cache Nodes

Software Library Storage

The Software Library Administration console allows you to configure and administer Software Library. To start using the Software Library, you must add at least one upload file storage location (OMS Shared File System, or OMS Agent File System) on the host where the OMS is running. A storage location in Software Library represents a repository of files that are either uploaded to Software Library or referenced by it.

Note

If you choose to newly configure an OMS Shared Storage Location, then ensure that the file system path that you specify for the location is either a shared path or a mounted path. By doing so, the newly configured location can be made accessible in a multiple OMS environment in the future. If the new location is being added in a multiple OMS environment, then the file system path should be accessible from all the OMS hosts.

However, if you have configured the OMS Shared Storage Location on a local file system, then perform the steps listed in the [Configuring Software Library Storage Location](#) to migrate this location to another OMS Shared Storage Location that has a shared or mounted path.

To access the administration console, log in to Enterprise Manager with Administration access, and follow these steps:

In Enterprise Manager, from the **Setup** menu, select **Provisioning and Patching**, and then click **Software Library**.

OR

In Enterprise Manager, from the **Enterprise** menu, select **Jobs and Procedures** and then, click **Software Library**. On the Software Library home page, from **Actions** menu, select **Administration**.

Software Library: Administration Page Refreshed Nov 18, 2015 11:24:19 AM UTC ↻

Software Library > Software Library: Administration

The administration console enables you to configure and administer the Software Library storage locations and cache nodes.

[Upload File Locations](#) | [Referenced File Locations](#) | [Cache Nodes](#)

Configure the storage locations that can be used for uploading files for Software Library entities.

Storage Type: OMS Shared File System

Configure file system locations on the OMS hosts. Make sure the locations are accessible by all the OMS instances, typically mounted or shared locations. You can optionally configure the common credential to be used by the Software Library for reading/writing from/to a location.

Actions ▼ View ▼ ➕ Add... ✎ Edit... ✕ Migrate and Remove

Name	Status	Location	Associated Entities	Credential	Total Space	Available Space	Used Space	Deleted Entities Used Space	Last Refreshed
swlib	Active	/nfs1c042b1/cratch/csadmin/swlib/	Show	Change Credential Clear credential	232.69 GB	153.58 GB	16.61 GB	0 Bytes	Nov 18, 2015 11:03:24 AM UTC

The Software Library Administration Page is a GUI based screen that enables you to create one or more storage locations to store or refer to files that are associated with an entity. To view the entities present in the storage location, click **show** on the Administration page. You can create a storage location on the OMS or the agent running on the same host as the OMS. Using the Referenced File Location, Software Library entities can refer to files that are stored on another host. These locations are however read-only for Software Library, and will not be used for uploading.

The space requirements for configuring Software Library depends on the amount of space required for storing the software binaries, and its associated scripts. Understandably, this space requirement increases over a period of time as you create more entities. Depending on the features or software required for provisioning and patching, you must decide and configure the Software Library storage space.

Note

For production environments, Oracle recommends allocating a minimum 100GB of storage for your software library. Also, ensure that this storage can easily be extended in future, if it starts running out of space.

Once the storage location starts running out of space, it is important to deactivate the configured storage location so that no new uploads can happen to this location. For more information about removing a storage location, see [Maintaining Software Library](#)

The following types of storage locations are available:

- [Upload File Locations](#)
- [Referenced File Location](#)
- [Cache Nodes](#)

Upload File Locations

Upload File Locations are locations configured for storing files uploaded by Software Library as part of creating or updating an entity.

For Software Library to become usable, at least one upload file location must be configured. On adding the first upload file location, a job is submitted to import the Software Library metadata from the Oracle home of each of the installed Enterprise Manager plug-in. Ensure that you wait for this job to complete successfully, before performing other patching or provisioning operations.

Note

To physically delete a file system configured as an Upload storage location with Software Library, you must ensure that you first configure an alternate storage location where you can migrate the existing contents (entities). If you fail to perform this migration, then the entities dependent on the files from this location will be rendered unusable. For more information about deleting a storage location, and migrating the contents, see [Removing \(and Migrating\) Software Library Storage Location](#).

Prerequisites

As a prerequisite, before using Upload File Locations as storage option, you must set credentials for using an OMS Shared File System or OMS Agent File System:

- For multiple OMS environment, all the OMS hosts must have a preferred normal host credential set.

When OMS instances are added, it is necessary to ensure that the configured locations are accessible from the designated host where the new OMS will be provisioned. For an OMS that will be provisioned using the Add Management Service functionality, the shared location configured as upload location should be mounted on the designated host, and verified manually.

- For OMS Agent File System location configuration, a credential (preferred or named) has to be specified.

Upload File Locations support two storage options as follows:

OMS Shared File System (Recommended Storage Option)

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.

Note

Oracle recommends using OMS Shared File System option for storing files uploaded to Software Library. However, if you are not able to set up a shared file system because of some constraints, then you may use the OMS Agent File System. For more information, see "[Upload File Locations](#)."

For single OMS environments, you can configure the Software Library either on the host where the OMS is running, or in a shared location. However, in future, if you plan to expand the single OMS setup to a multiple OMS setup, then local file system path is not recommended.

Note

For a multi-OMS scenario, you must set up clustered file system using NFS or DBFS. On Windows, for sharing, the OCFS2 cluster file system is recommended.

If you are implementing multiple management servers for high availability you should also make the Software Library file system highly available. Besides accessibility and availability, it is important to ensure that there is enough space (more than 100 GB for production deployment of Enterprise Manager) available for the storage of software binaries, and associated scripts for the entities that you want to create and store.

OMS Agent File System

An OMS Agent File System location should be accessible to the agent running on the host machine where the OMS is deployed. To use OMS Agent File system storage option, ensure that you have a preferred, or a named credential for the OMS host. Click **Change Credential** to change the associated credential to be used to access this location.

Note

If you can not set up an OMS Shared File System for storage because of some constraints, then you may use the OMS Agent File System.

Referenced File Location

Referenced File Locations 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:

- **HTTP:** An HTTP storage location represents a base URL which acts as the source of files that can be referenced.

For example, the base URL <http://my.files.com/scripts> could be configured as an HTTP location for sourcing files such as <http://my.files.com/scripts/perl/installMyDB.pl> or <http://my.files.com/scripts/linux/stopMyDB.sh>.

- **NFS:** An NFS storage location represents an exported file system directory on a server. The server need not be an Enterprise Manager host target.

For example, the directory `/exported/scripts` is exported on server `my.file.server` could be configured as an NFS location for sourcing files such as `/exported/scripts/generic/installMyDB.pl` or `/exported/scripts/linux/stopMyDB.sh` once mounted on a target host file system.

- **Agent:** An Agent storage location is similar to the OMS Agent File System option, but can be any host monitored by an Enterprise Manager Agent. The Agent can be configured to serve the files located on that host.

For example, the directory `/u01/binaries` on the Enterprise Manager Host `my.em.file.server` could be configured as an Agent location for sourcing files such as `/u01/binaries/rpms/myCustomDB.rpm` or `/u01/binaries/templates/myTemplate.tar.gz`.

These locations require a named credential to be associated which will be used to access the files from the base location on the host through the Enterprise Manager Agent.

Note

To use entities referring files of a location, you must have view privilege on the credentials associated with the locations.

Cache Nodes

Cache Nodes is a feature in Enterprise Manager that enhances the file transfer experience to distant servers and data centers by reducing the load on the OMS. Cache nodes work on a set of predefined targets that function as one unit called the Group, and each cache node is an intermediate storage location on a host that serves a particular group of targets that it is associated with. For more information about Cache Nodes, see [Configuring the Cache Nodes](#)

Prerequisites for Configuring Software Library

To administer the different storage types, and to configure software library, keep the following points in mind:

- Depending on the features or software required for provisioning and patching, you must decide and configure the Software Library storage space. The storage needs change based on the usage pattern.
- Each OMS host must have a preferred normal host credential set before configuring the location. For OMS Agent File System location configuration, a credential (preferred or named) has to be specified.
- You (the user configuring the Software Library) must have view privilege on all the OMS, and the agent targets running on the host machine. As per the accessibility verification, you must be able to view, and edit these newly configured locations.

- To add an OMS Agent storage location, ensure that you have view privileges on the target OMS host, and the agents running on that target host.

Configuring Software Library Storage Location

System Administrators are responsible for configuring a storage location. Only after the storage location is configured, you can start uploading the entity files.

Note

Deployment procedures and area-specific jobs in your on-prem Cloud setup may in turn use entities like Components and Directives from the Software Library for managing Oracle Cloud targets. For your procedure to successfully manage the Oracle Cloud targets, Software Library must be configured to use an OMS Shared File system storage for the uploaded files. If these Components and Directives use OMS Agent File system storage, the procedure will fail when attempting to transfer the files to the Oracle Cloud targets.

You can configure the Software Library in one of the following locations:

- [Configuring an OMS Shared File system Location](#)
- [Configuring an OMS Agent File system Location](#)
- [Configuring a Referenced File Location](#)

Configuring an OMS Shared File system Location

To configure an OMS Shared File System storage location that can be used for uploading Software Library entity files, perform the following steps:

1. From the **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library: Administration page, select **OMS Shared File system**.
3. To add a new OMS Shared File System, click **+Add**.
4. In the Add OMS Shared File System location dialog box, provide a unique name, host name, and location on the OMS host, where you want to set up the upload location.

Add OMS Agent File System Location X

Provide a name, a host, and a file system location on the host. The host can only be one of the hosts where the OMS is running. The credential used for selecting the file system location on the host will be copied into a secure system credential and saved along with this location.

* **Name** omsagent1

Host blr2202394.idc.oracle 🔍

Location /scratch/agent1 🔍

OK Cancel

Providing Credentials is optional. If you provide, then it will be used for transferring files.

Ensure that the configured storage location is a shared location that is accessible by all the OMS instances. For a Multi OMS setup, set the Normal Preferred Credentials for all the OMS(s).

When you configure an upload location for the first time, a metadata registration job is submitted which imports all the metadata information of all the installed plug-ins from the Oracle home of the OMS.

To track the progress of the job, click **Show Detailed Results**. Typically, the name of the job starts with `SWLIBREGISTERMETADATA_*`.

If the Import job fails, see [Maintaining Software Library](#) for information on Re-importing metadata for Oracle-owned files.

5. Click **OK** to create a new entry for the storage location in the table, with details like **Name**, **Location**, **Host**, **Status**, and **Host Credentials**.

In addition to this, you can click **Associated Entities** to view or search the entities present in the selected upload location.

Configuring an OMS Agent File system Location

Note

The OMS Agent File system must be set up only when the recommended storage option, which is the OMS Shared File System cannot be set up because of some constraints. For more information, see [Upload File Locations](#).

To configure an OMS Agent location, perform the following steps:

1. From the **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library: Administration page, select **OMS Agent File system**.

Add OMS Agent File System Location ✕

Provide a name, a host, and a file system location on the host. The host can only be one of the hosts where the OMS is running. The credential used for selecting the file system location on the host will be copied into a secure system credential and saved along with this location.

* **Name**

Host 🔍

Location 🔍

OK **Cancel**

3. Click **+Add**, in the Add OMS Agent File System Location dialog box, enter the following details:
 - a. In the **Name** field, enter a unique name for the storage.
 - b. In the **Host** field, click the magnifier icon. From the Search and Select: Hosts dialog box, select a host where the OMS is running, and click **Select**.
For example, `xyz.mycompany.com`
 - c. In the **Location** field, click the magnifier icon. In the Remote File Browser dialog box, click **Login As** to log in to the host machine with either Preferred, Named or New credentials.

Note

For a user to access and leverage an OMS Agent File system upload location successfully, the owner of the Named Credential (basically, the credential used to connect to the host machine), must grant a View Privilege on the credential chosen to all the Administrators (or users) accessing this OMS Agent File system location.

For more information about granting privileges on a Named Credential, refer to *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

Navigate to the location on the host where you want to create the Agent File System, and click **OK**.

The selected credential is saved along with the host and selected file system path. The saved credential is used to upload files and stage the uploaded files to a host target as part of some provisioning or patching activity.

Note: The credential is copied into a system owned credential with a generated name that starts with SWLIB. This will appear as the original credential name during Edit Credential flow.

4. Click **OK** to create a new entry for the storage location in the table, with details like **Name**, **Location**, **Host**, **Status**, and **Host Credentials**.

In addition to this, you can click **Associated Entities** to view or search the entities present in the selected upload location.

These newly configured OMS Agent locations are now available for storing entity files.

Configuring a Referenced File Location

To configure storage location that can be used for referring to files from the Software Library entities, perform the following steps:

1. From the **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library: Administration page, click **Referenced File Locations** tab.
3. To add an HTTP location that can be accessed through a HTTP URL, select **HTTP** from the Storage Type list and click **+Add**.

In the Add HTTP Location dialog box, enter a unique name and a HTTP location for the storage that you want to reference, and click **OK**.

A new entry for the storage location is created, with details like **Name**, **Location**, and **Status**.

4. To add an NFS shared location, select **NFS** from the Storage Type list and click **+Add**.

In the Add NFS Location dialog box, do the following:

- a. Enter a unique name in the **Name** field for the storage.
- b. In **NFS server** field, provide a fully qualified domain name or the IP address of the hosted machine that has NFS services running on them.
- c. In the **Location** field, provide the shared location or directory path on the NFS server to define a storage location, then click **OK**.

A new entry for the storage location is created in the table, with details like **Name**, **Location**, and **Status**.

Note

While creating a procedure, if you have a component step or a directive step that refers to an NFS file location, then you must ensure that you set the preferred privileged credentials for the target host before the procedure is submitted for execution.

5. To add an Agent location that has read-only privileges set on it, select **Agent** from the Storage Type list and click **+Add**.

In the Add Agent Location dialog box, enter the following details:

- a. In the **Name** field, enter a unique name for the storage.
- b. In the **Host** field, click the magnifier icon to select a target from the list available.
For example, `xyz.mycompany.com`
- c. In the **Location** field, click **Login As** to select the credentials and browse the previously selected host.

The credential selected, either Preferred, Named or New, is saved along with the host and selected file system path. The saved credential is used for staging the files to a host target as part of some provisioning or patching activity.

Note: The administrator configuring the Software Library must grant view privilege (at least) on the credential chosen to all designers uploading or staging the files to or from this location.

Note: When you create a new entity, these newly configured Referenced File Locations are available as storage options.

Configuring Software Library on a Multi-OMS System

Oracle recommends that you configure each OMS Shared Storage Location to use a shared or mounted file system path. Doing this will ensure that this newly configured location remains accessible from any OMS host as and when they are added. All upload and stage requests for the files will happen through the Management Agent monitoring the OMS host.

Note

Use the EM CLI utility to migrate files across upload locations of different storage types. To migrate files from an OMS Shared storage location to an OMS Agent storage location, use the EM CLI verb `remove_swlib_storage_location`. The same verb supports the reverse action as well. Alternatively, you can also use the Enterprise Manager UI. For information about how to use Enterprise Manager to migrate files across storage locations, see [Removing \(and Migrating\) Software Library Storage Location](#).

If however, you have configured the OMS Shared storage location to use a local file system path, then you must migrate it to another OMS Shared Storage Location that uses a shared or mounted path. To do so, follow these steps:

1. In the Enterprise Manager console, from **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library Administration page, add a new OMS Shared storage location by specifying a name (for example: NewShared), and a shared file system path.
3. On successful completion, select the location you want to migrate, (For example: OldNonShared), and click **Migrate and Remove**.
4. In the pop-up dialog box, select the new OMS Shared File System as the storage plugin type, and the new OMS shared storage location (NewShared) as the destination to migrate the files.
5. Click **Remove** to submit a job, which on successful completion deletes the storage location entry from the table.

Software Library Cache Nodes

Enterprise Manager supports configuring one or more cache nodes in close proximity to a group of targets. Once configured, the Software Library File Transfer job ensures that entity files are picked from the appropriate cache node, caching the entity files as needed, thereby reducing the time taken for transferring files to targets distant from the Oracle Management Service.

Configuring the Cache Nodes

Cache Nodes is a feature in Enterprise Manager that enhances the file transfer experience to distant servers and data centers by reducing the load on the OMS. Cache nodes work on a set

of predefined targets that function as one unit called the Group, and each cache node is an intermediate storage location on a host that serves a particular group of targets that it is associated with.

Typically, creating a group with targets that belong to the same geographical location is beneficial. Proximity of these targets ensures efficient file transfers. Having a cache node is also hugely beneficial to reduce the load on the OMS. For example, patching 100 targets at the same time is a huge load on the OMS, as the OMS will have to orchestrate file transfers with each of the 100 targets individually. However, you can counter this by using cache nodes in a way that the OMS just needs to transfer the files to the cache node once, and the cache node in turn processes the file transfer to the individual targets in the group that it is serving. Note that a given group of targets can be linked to more than one cache node. This approach is employed to ensure that the load is equally balanced across the nodes, which in turn helps in maximizing the performance of the individual cache node of the associated group.

In particular, this section covers the following:

- [Adding Cache Nodes](#)
- [Editing the Cache Nodes](#)
- [Deleting the Cache Nodes](#)
- [Activating or Deactivating the Cache Nodes](#)
- [Clearing the Cache Nodes](#)
- [Synchronizing the Cache Nodes](#)

Adding Cache Nodes

Note

The credential is copied into a system owned credential with a generated name that starts with SWLIB. This will appear as the original credential name during the Edit Credential flow.

Before you begin adding cache nodes, you must ensure that you have created a group of targets to associate with the relevant cache nodes. For information on creating groups, see [Managing Groups](#).

To add cache nodes, follow these steps:

1. In Enterprise Manager, from the **Setup** menu select **Provisioning and Patching**, then click **Software Library**.
2. On the Software Library Administration page, select **Cache Nodes**.
3. On the Cache Node tab, click **Add**.

Add Cache Node [X]

Create a new cache node to serve targets in a group

* **Name**

Description

* **Host** [Search]

* **Location** [Search]

* **Group** [Search]

* **Quota (GB)**

[OK] [Cancel]

4. In the Add Cache Node dialog box, enter the following details:
 - a. Enter a display name for the cache node. For example: Austin Nodes.
 - b. Add a short description for the cache node for your reference. For example, these are the targets on different hosts restricted to Austin, U.S.A.
 - c. Provide the host target machine that will be used as the cache node. For example, slc01.example.com
 - d. Provide a location on the host to store the files that are transferred from the OMS. Note that the directory must already exist and must be empty. For example, `/usr/cachenodes`
 - e. Search and select the group to be associated with the cache node. For example, Austin Group.
 - f. Quota by default is 10 GB, you can change this value and customize it to your requirement.
5. Click **OK** to create a cache node that serves the targets added to the group specified.

A summary of the available disk space, the file transfer history, and the information about the cache node is displayed once the node is successfully created.

Once the cache node is successfully created, you can click show to view all the entities associated with the targets in the group. Additionally, you can view the group details by clicking the group name.

Editing the Cache Nodes

To edit cache nodes, follow these steps:

1. In Enterprise Manager, from the **Setup** menu select **Provisioning and Patching**, then click **Software Library**.
2. On the Software Library Administration page, select **Cache Nodes**.
3. On the Cache Node tab select the cache node that you want to update, and click **Edit**. This is particularly useful when you want to change the group associated with the cache or update the quota details.
4. Click **OK** to reflect the changes.

Deleting the Cache Nodes

To remove a cache, follow these steps:

1. In Enterprise Manager, from the **Setup** menu select **Provisioning and Patching**, then click **Software Library**.
2. On the Software Library Administration page, select **Cache Nodes**.
3. On the Cache Node tab select one or more cache nodes, and click **Delete**.

Activating or Deactivating the Cache Nodes

If you want to temporarily suspend the functioning of a particular cache node, click **Deactivate**. Typically, when the quota is full or when you have to carry out some maintenance tasks on the cache nodes, this option becomes useful.

To deactivate a cache node, follow these steps:

1. In Enterprise Manager, from the **Setup** menu select **Provisioning and Patching**, then click **Software Library**.
2. On the Software Library Administration page, select **Cache Nodes**.
3. On the Cache Node tab select a cache node, and click **Deactivate**.

Clearing the Cache Nodes

If you want to remove all the files associated with a cache node in order to free up the quota, click **Clear**.

To clear a cache node, follow these steps:

1. In Enterprise Manager, from the **Setup** menu select **Provisioning and Patching**, then click **Software Library**.
2. On the Software Library Administration page, select **Cache Nodes**.
3. On the Cache Node tab select a cache node, and click **Clear**.

Synchronizing the Cache Nodes

To identify and clean up the inconsistencies within the cache node, follow these steps:

1. In Enterprise Manager, from the **Setup** menu select **Provisioning and Patching**, then click **Software Library**.
2. On the Software Library Administration page, select **Cache Nodes**.
3. On the Cache Node tab select a cache node, and click **Resynchronize**.

Exporting and Importing Files for Cache Nodes

EM CLI verbs are available for exporting Software Library entities' files into compressed files. These compressed files can be transported to a cache node host and imported into the cache node. If Software Library entities are staged to one or more targets in the group served by the cache node, then the files will be served directly from the cache node in place of the OMS.

Export

Create a file with one Software Library entity internal ID per line. The internal ID of entities can be revealed by `emcli verb list_swlib_entities`. The file `/u01/urnfe` in the following example is such a file. Files of entities represented by lines in this file will be exported as `/u01/exportcache/cachefiles.zip` on host `syq.myco.com`, using credential named `creds1` owned by the Enterprise Manager user `ADMIN1`.

```
emcli export_swlib_cache_files -dest_dir_path=/u01/exportcache -  
zip_file_name=cachefiles.zip -dest_host_name=syq.myco.com -  
urn_file_entry_file="/u01/urnfe" -dest_host_tmp_dir=/tmp -credential_name=creds1  
-credential_owner=ADMIN1
```

Once the file `cachefiles.zip` has been exported, it can be taken to the intended destination cache node, such as `skx.af.myco.com`.

Import

The zip file can now be imported into the cache node using the following `emcli` verb: `emcli import_swlib_cache_files -src_dir_path=/u01/cachefiles -zip_file_name=cachefiles.zip -cache_node_name=afcacachenode -src_host_tmp_dir=/tmp -src_host_name=skx.af.myco.com`

The credential associated with the cache node will be used for performing the import.

For more details, see Oracle Enterprise Manager command line interface guide.

Software Library File Transfers

The Software Library File Transfer jobs submitted as part of different provisioning/patching procedure/job runs can be searched and viewed from the File Transfer Activity page.

File Transfer Activity Page

The File Transfer Activity page enables you to track file transfers related to Software Library.

To access this page, log in to Enterprise Manager and from the **Enterprise** menu, select **Jobs and Procedures**, then click **Software Library**. On the Software Library home page, from the Actions menu, select **File Transfer Activity**.

The table on this page shows all file transfer activities that have been performed recently. The **Job Name** column displays the job for which the file transfer activity was performed, and the **Procedure Run Name** column displays the Deployment Procedure run name if it is run within a Deployment Procedure. Both these columns together can be used to identify the file transfer activity.

Using Software Library Entities

To access the Software Library Home Page, in Enterprise Manager, from the **Enterprise** menu, select **Jobs and Procedures** and then click **Software Library**. Software Library is a repository that stores certified software binaries such as software patches, virtual appliance images, reference gold images, application software and their associated directive scripts, generally referred to as *Entities*. Accesses and privileges on these entities are decided by the Super Administrators or the owner of the entity.

Entities can broadly be classified as:

Types	Description
Oracle-owned Entities	These entities are available by default on the Software Library Home page, once the Software Library is configured. In the following graphic, all the entities that are owned by Oracle , qualify as Oracle-owned entities, and all the folders that appear with a lock icon against them are Oracle-owned folders like Application Server Provisioning, Bare Metal Provisioning, Cloud, and so on.
Custom Entities	These entities are created by the Software Library users. For example, in the following graphic you can see a custom folder called My Entities, and entities called os2 and os1 created by the owner of the entity. These entities are called User-owned entities.

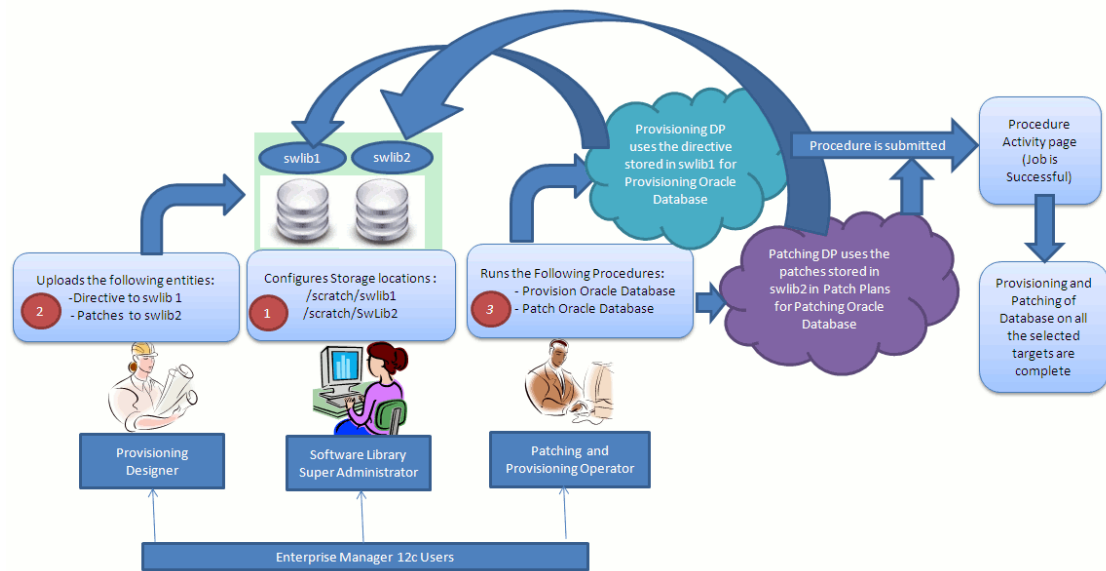
Name	Type	Subtype	Revision	Status	Maturity	Owner	Description
Software Library						ORACLE	Root Folder for Software Library entities
Application Server F						ORACLE	Entities belonging to AS Provisioning
Bare Metal Provision						ORACLE	Bare Metal Provisioning directory
BPELProvisioning						ORACLE	BPEL Provisioning Entities
Cloud						ORACLE	Cloud
Coherence Node Pr						ORACLE	Coherence Node Provisioning Entities
Common Provisionir						ORACLE	Directives belonging to Common Provisionin
Components						SYSMAN	Components Folder
Directives						SYSMAN	Directives Folder
Images						SYSMAN	Images Folder
Networks						SYSMAN	Networks Folder
Suites						SYSMAN	Suites Folder

Note

All Oracle-owned folders (and entities) are available on the Software Library Home page by default. The Oracle-owned folders have a read-only privilege, so you cannot select these folders to create an entity. You must create a custom folder to place your entities in them.

A number of lifecycle management tasks such as patching and provisioning deployment procedures make use of the entities available in Software Library to accomplish the desired goal. Here is a pictorial representation of how a Provisioning Deployment Procedure and a Patching Deployment Procedure makes use of the entities available in the Software Library:

Figure 3-2 Using Software Library Entities for Provisioning and Patching Tasks



Tasks Performed Using the Software Library Home Page

From the Software Library Home page, you can do the following:

- [Organizing Entities](#)
- [Creating Entities](#)
- [Customizing Entities](#)
- [Managing Entities](#)
- [Staging Entities](#)

Organizing Entities

Only designers who have the privilege to create any Software Library entity, can create folders.

To create a custom folder, perform the following steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, and then select **Software Library**.
2. On the Software Library Home page, from **Actions** menu, click **Create Folder** to create a custom folder of your own.

The custom folder can contain User-owned folders, entities, and customized entities created by using the *Create Like* option.

3. In the Create Folder dialog box, enter a unique name for the folder. Also, select the parent folder in which you want to create this new custom folder and click **Save**.

For example, if the root folder is `Software Library` and you created a custom folder in it called `Cloud12gTest`, then the Parent Folder field is populated as follows: `/Software Library/Cloud12gTest`.

Note: Only the owner of the folder or the Super Administrator has the privilege to delete the folder, nobody else can.

Creating Entities

From the Software Library Home page, you can create the following entities:

- [Creating Generic Components](#)
- [Creating Directives](#)

Creating Generic Components

To create a generic component from the Software Library Home page, perform the following steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. On the Software Library Home page, select a custom folder that is not owned by Oracle.
Note: You cannot create a generic component in an Oracle Owned Folder. To create a custom folder, see [Organizing Entities](#).
3. From the **Actions** menu, select **Create Entity** and click **Component**. Alternately, right click the custom folder, and from the menu, select **Create Entity** and click **Component**.
4. From the Create Entity: Component dialog box, select **Generic Component** and click **Continue**.

Enterprise Manager displays the Create Generic Component: 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 such as 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, you can customize the generic component that you are creating by adding some new properties or updating the existing properties of the component.

Note: Select **Shared Type** to reuse the component property. Shared Type can be stored as a template, which can be used for creating different and more complicated top level types.

To add a new property, do the following, and click **Next**:

- a. Select **Top Level Type** or **Shared Type**, and click **Add**.
- b. Enter a unique name for the property. Depending on the property type selected, enter an initial or default value for the property.
- c. To add a constraint, specify the Minimum or Maximum value for the selected property type, and click **Add Constraint**.

The Configured Constraints table lists all the constraints added. To remove a particular constraint from the property, select the property and click **Remove**.

7. On the Select Files page, you can select one or more files to be associated with the entity. Select one of the following options:

- **Upload Files:** If you want to upload some entity files from the local file system or the agent machine to the selected destination location.

To select the destination location, in the Specify Destination section, in the **Upload Location** field, click the magnifier icon to select one of the following options:

- **OMS Shared File System**
- **OMS Agent File System**

The corresponding Storage Type and Location Path of the selected location is populated.

Note

To upload the files, the status of the storage location to which the files are to be uploaded should be **Active**.

If you select OMS Agent File system location, then ensure that you have the necessary privileges to access the location

In the Specify Source section, enter the location from where the files are being sourced, these locations can either be local file system or a remote file system monitored by the Management Agent. Select one of the following options for File Source:

- If you select **Local Machine**, and click **Add**, the Add File dialog box appears. Click **Browse** to select the entity file from the source location, and give a unique name, and click **OK**.

You can upload the files to any of the configured storage locations available in OMS Shared File system location or OMS Agent File system location

- If you select **Agent Machine**, select the name of the host machine from where you want to pick up the entity files. Click **+Add** and log in to the host machine with the desired credentials. For more information about the different credential types and their setup, see the *Oracle Enterprise Manager Lifecycle Management Guide*.

Once you log in to the host machine, browse to the location where the files to be uploaded are present. You can upload the files to any of the configured storage locations available in OMS Shared File system location or OMS Agent File system location.

- **Refer Files:** If you select the **Refer Files** option, you only need to enter the source location details, since you are not technically uploading anything to the Software Library. In the Specify Source section, select from **HTTP**, **NFS**, or **Agent Storage** types, and click OK. The corresponding Storage Type and Location Path of the selected location is populated.

Click **+Add** to reference the entity present at the selected Referenced File Location. In the Add Referenced File dialog box, enter a relative path to the file under Base Location. Click **Stage As** to organize the file in a temporary stage location with a unique name.

For details about each of these storage options, see [Configuring a Referenced File Location](#)

8. On the Set Directives page, click **Choose Directives** to associate a component with one or more directives. Click **Next**.

9. On the Review page, review all the details, and click **Finish** to create the component and upload it on the Software Library.

Creating Directives

Directives are entities in the Software Library that represent a set of instructions to be performed. These are constructs used to associate scripts with software components and images. These scripts contain directions on how to interpret and process the contents of a particular component or an image.

To create a directive from a Software Library Home page, perform the following steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. On the Software Library Home page, select a custom folder that is not owned by Oracle.
Note: You cannot create a generic component in an Oracle Owned Folder. To create a custom folder, see [Organizing Entities](#).
3. From **Actions** menu, select **Create Entity** and click **Directive**. Enterprise Manager displays the Create Entity: Directives wizard.
4. 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. In case you enter a unique name and it reports a conflict, it may be due to 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 such as 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.

5. On the Configure page, specify the command line arguments that must be passed to the directive to configure it. This command provides the parameters required to execute the directive.

To add the command line arguments or parameters, click **Add**.

In the Add Command Line Arguments dialog box, enter the values in the following fields:

- **Argument Prefix**, is a switch or a constant command line argument.

The Argument Prefix eliminates the error-prone task of manually specifying the order of the parameter executions in a given directive. This is specially useful when a directive is made of multiple parameters.

Oracle recommends that you create command line arguments using an Argument Prefix.

- **Property Name**, is the name of the property, that must be a string value.
- **Argument Suffix**, is the text that must follow the command line property.

Though the suffix is rarely used, it determines how the parameters must be executed, based on the suffix value.

For example, if the command line argument you want to pass is as follows:

```
./test.sh -user={username}
```

Then,

Argument Prefix is: `-user`

Property Name is: username

All the parameters added appear in the order of addition against the **Command Line** field.

To change the order of the parameter or edit any property of an existing parameter, click **Edit**.

To remove any of the parameters, click **Remove**.

In the Configuration Properties section, select either **Bash** or **Perl** as defined in the script.

Select **Run Privileged** to run the script with `root` privileges.

6. On the Select Files page, you can select one or more files to be associated with the entity. Select one of the following options:

- **Upload Files:** If you want to upload some entity files from the local file system or the agent machine to the selected destination location.

To select the destination location, in the Specify Destination section, in the **Upload Location** field, click the magnifier icon to select one of the following options:

- **OMS Shared File System**
- **OMS Agent File System**

The corresponding Storage Type and Location Path of the selected location is populated.

 **Note**

To upload the files, the status of the storage location to which the files are to be uploaded should be **Active**.

If you select OMS Agent File system location, then ensure that you have the necessary privileges to access the location.

In the Specify Source section, enter the location from where the files are being sourced, these locations can either be local file system or a remote file system monitored by the Management Agent. Select one of the following options for File Source:

- If you select **Local Machine**, and click **Add**, the Add File dialog box appears. Click **Browse** to select the entity file from the source location, and give a unique name, and click **OK**.

You can upload the files to any of the configured storage locations available in OMS Shared File system location or OMS Agent File system location

- If you select **Agent Machine**, select the name of the host machine from where you want to pick up the entity files. Click **+Add** and log in to the host machine with the desired credentials. For more information about the different credential types and their setup, see the *Oracle Enterprise Manager Lifecycle Management Guide*.

Once you log into the host machine, browse to the location where the files to be uploaded are present. You can upload the files to any of the configured storage locations available in OMS Shared File system location or OMS Agent File system location.

- **Refer Files:** If you select the **Refer Files** option, you only need to enter the source location details, since you are not technically uploading anything to the Software Library. In the Specify Source section, select from **HTTP**, **NFS**, or **Agent Storage**

types, and click OK. The corresponding Storage Type and Location Path of the selected location is populated.

Click **+Add** to reference the entity present at the selected Referenced File Location. In the Add Referenced File dialog box, enter a relative path to the file under Base Location. Click **Stage As** to organize the file in a temporary stage location with a unique name.

For details about each of these storage options, see [Configuring a Referenced File Location](#)

7. On the Review page, review all the details, and click **Finish** to create the component and upload it on the Software Library.

Customizing Entities

You cannot edit an entity present in an Oracle owned folder. However, to edit an Oracle-owned entity, you can make a copy of the entity and store it in a custom folder. Since you now have full access on the entity, you can customize the entity based on your requirement and may even choose to grant other users access to this entity.

To create a custom entity from an Oracle owned entity, perform the following steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. On the Software Library Home page, select an entity or alternately, search and select an entity.

For more information about searching for an entity, see [Searching Entities](#).

3. From **Actions** menu, select **Create Like**.
4. On the Create Like: <Entity Name> dialog box, enter a name that is unique to the parent folder and a description for the entity.

By default, the root directory Software Library is preselected in the **Parent Folder** field.

To change the parent folder and organize the entities, click **Change Parent Folder**. and select the desired folder.

5. Click **OK** to apply the changes.

The new entity appears in the Entities table, under the selected parent folder.

You as the owner have all the privileges on the entity, and can update the properties as per your requirement.

To update the properties of the entity, see [Viewing, Editing, and Deleting Entities](#).

For more information on Oracle Owned Entities and User Owned Entities, see [Using Software Library Entities](#).

Managing Entities

From the Software Library Home page, you can perform the following maintenance tasks on the existing entities:

- [Accessing Software Library Home Page](#)
- [Accessing Software Library Administration Page](#)
- [Granting or Revoking Privileges](#)
- [Moving Entities](#)

- [Changing Entity Maturity](#)
- [Adding Notes to Entities](#)
- [Adding Attachments to Entities](#)
- [Viewing, Editing, and Deleting Entities](#)
- [Searching Entities](#)
- [Exporting Entities](#)
- [Importing Entities](#)

Accessing Software Library Home Page

To access the Software Library Home page, from the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.

Accessing Software Library Administration Page

To access the Software Library Administration page, from the **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.

Granting or Revoking Privileges

An Enterprise Manager user requires, at the very least, a view privilege on an entity for the entity to be visible on the Software Library Home. The owner or super administrator can choose to grant additional privileges like edit (Update notion) or manage (or full) or at a later point of time, revoke the previously granted privilege.

To grant or revoke privileges, perform the following steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. To grant or revoke fine-grained privileges to the other users on any entity that you own, select the custom entity and from **Actions** menu, click **Grant/Revoke Privileges**.
3. On Grant/Revoke Privileges on: <entity_name> window, you can either grant or revoke Software Library privileges depending on the users roles and responsibilities in the organization.

Granting Privileges: To grant one or more new privileges, click **+Add** and search for the users. You can grant them one of the following privileges on the entity you own:

- **View Software Library Entity:** This is normally an operator privilege where the user can only view the entity on the Software Library Home. The user cannot edit or manage the entity. All the Oracle owned entities can be viewed by all Enterprise Manager users.
- **Edit Software Library Entity:** This is a designer privilege where a user has Create, Update, and Edit privileges on the entity.
- **Manage Software Library Entity:** This is a super-administrator privilege where the user has complete access on the entity. With this privilege, you can grant or revoke accesses on this entity to other users, or delete the entity.

Revoking Privileges: To revoke previously granted privileges, select the user and click **Remove**.

4. Click **Update** to apply the selected grants on the entity.

Moving Entities

To move all the revisions of an entity from one folder to another, do the following:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. On the Software Library Home page, select an entity or alternately, search and select an entity.

For more information about searching for an entity, see [Searching Entities](#).

3. From the **Actions** menu, click **Move Entity** and accept the confirmation.
4. From the Move Entity dialog box, select the destination folder for the entities and click **Set New Parent Folder**.

Note: Ensure that the source and the destination folders are not owned by Oracle, as you cannot move or edit them.

Changing Entity Maturity

When an entity is created from the Enterprise Manager Home, it is present in an Untested state. It is the responsibility of a designer to test the entity, and change the maturity level based on the test result.

To manage the lifecycle and indicate the quality (maturity level) of an entity, perform the following steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. On the Software Library Home page, select an entity or alternately, search and select an entity.

For more information about searching for an entity, see [Searching Entities](#).

3. From the **Actions** menu, click **Change Maturity** to change the maturity value an entity after testing.

For example, an Oracle Database Clone component would be tested by selecting it in a deployment procedure interview flow that provisions a database. Once the entity is tested, the designer can change the maturity of the entity to either Beta or Production based on test results. Only when the entity is marked with Production level, the Operator can use it.

Adding Notes to Entities

To log information about the changes or updates made to an existing entity, perform the following steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. On the Software Library Home page, select an entity or alternately, search and select an entity.

For more information about searching for an entity, see [Searching Entities](#).

3. From **Actions** menu, click **Notes** to include any important information related to the entity. You can also add notes while editing an entity.

The most recent note appears on top of the table, and the older notes appear below.

4. After updating the details, click **Finish** to submit the changes, and return to the Software Library Home page.

Adding Attachments to Entities

To add or upload files that are typically documents (like README, installation, configuration) related to the software the entity represents, perform the following steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. On the Software Library Home page, select an entity or alternately, search and select an entity.

For more information about searching for an entity, see [Searching Entities](#).

3. From **Actions** menu, click **Attachments** to include one or more files related to the entity. These files contain some important information about the entity. You can also attach files while editing an entity.

For example, you can attach a readme file to a patch or a component, attach a test script to a directive and so on. However, you must ensure that the file size of each attachment is not more than 2 MB.

4. Click **Finish** to submit the changes, and return to the Software Library Home page.

Viewing, Editing, and Deleting Entities

To view, edit, or delete the details of an entity, perform the following steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. On the Software Library Home page, select an entity or alternately, search and select an entity.

For more information about searching for an entity, see [Searching Entities](#).

3. To manage an existing entity, select the entity and perform any of the following functions:
 - **View:** Click **View** icon on the table to view the details of an entity. You cannot update the properties of the entity from here.
 - **Edit:** Click **Edit** icon on the table or right-click the entity and select **Edit** from the context menu to update the properties of an entity.

If you are satisfied with the details, click **Save and Upload** to make the changes available on the Software Library Home page.

- **Delete:** Click **Delete** icon to remove the entity from the Software Library Home page.

Note: By deleting an entity, the entity is no longer available for selection, viewing, or editing, and will not be displayed on the Software Library Home page. However, the entity continues to exist in the repository and the associated files, if uploaded, continue to exist in the respective disk storage. To delete the entity completely from the repository and the associated files from the file system, you must purge the deleted entities from the administration page. The purge job not only deletes the files associated with the deleted entity, but removes the deleted entities itself from the repository tables.

For more information about how to purge the deleted entities from the storage location, see [Purging Deleted Entities](#).

Purging Deleted Entities

Note

Entities can be purged using the EMCLI verb `delete_swlib_entity`. See `delete_swlib_entity` in the *Enterprise Manager Command Line Interface Guide* for more information.

To purge the deleted entities from all the configured Agent Storage locations, you can run a purge job. To do so, follow these steps:

1. In Enterprise Manager, from the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. On the Software Library home page, from **Actions** menu, select **Deleted Entities**. A list of entities that are deleted from Software Library are displayed.

Note

The **Space Used** attribute is displayed only for the deleted entities that had uploaded files to Software Library.

3. On the Deleted Entities page, click **Purge** to permanently remove these entities from Oracle Management Repository, and the associated files from upload storage locations.
4. A Confirmation Message dialog box is displayed. Click **Job Details** to view the status of the purge job submitted.

Note

A periodic job named `SWLIBPURGE` runs daily to purge the deleted entities from the Software Library.

Searching Entities

This section contains the following topics:

- [Performing Basic and Advanced Searches](#)
- [Saving Searches](#)
- [Retrieving Saved Searches](#)
- [Managing Saved Searches](#)

Performing Basic and Advanced Searches

To perform a basic or an advanced search for an entity, follow these steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. To search for an entity, perform one of the following operations:

- a. **Find:** On the Software Library Home page, you can search for an entity by its **Name**, **Description**, or **Type**. Select the search category, enter the desired value and then click the arrow icon.

On clicking the arrow icon, the result page displays a number of matching results, and allows you to toggle between the result rows by clicking the up and down arrows.

- b. **Search:** To perform a detailed search for an entity, click **Search**. The search option, by default, allows you to search by **Type**, **Name**, **Description**, **Revision**, **Maturity**, **Status**, and **File Name** to retrieve a more granular search result.

Note: If you choose entities that have associated subtypes (like Components), then the page is refreshed with **Subtype** as an additional search category.

Specify appropriate values in **All** or **Any** of the search fields, and click **Search**.

To add more search parameters, in the Advanced Search section, click **Add Fields** menu and, select the desired search fields. The selected fields appear in the Advanced Search section as new search parameters. This new search feature enables you to refine your search, and drill down to the most accurate and desired search result.

To revert to the simple search view, click **Close Search**.

Saving Searches

Optionally, search criteria on the Advanced Search screen of the console, can be saved. Saved searches can be retrieved and executed again. They can also be edited and deleted.

1. Search for entities.
2. Click **Save Search**.
3. Enter the preferred name for the search in the text box, and click **Ok**.

Retrieving Saved Searches

To retrieve saved searches, follow these steps:

1. Search for entities.
2. Click **Saved Searches**, and select the preferred saved search from the list.

Alternatively, you can also select the preferred saved search from the Favorites menu. To do so, from the **Favorites** menu, select **Saved Software Library Searches**, and select the preferred saved search.

Managing Saved Searches

Using the Manage Saved Searches option, you can edit the name of the saved search, or delete the saved search. To do so, follow these steps:

- To manage saved searches, you can perform one of the following steps:
 - From the **Favorites** menu, select **Manage Favorites**.
 - Click **Saved Searches**, and select **Manage Saved Searches**.
- To edit the name of the saved search, select the preferred saved search, and in the **Name** text field, enter the new name. Click **Ok** to save changes.
- To delete or remove a saved search, select the preferred saved search, and click **Remove Selected**. Click **Ok** to save changes.

Exporting Entities

To export selected entities, perform the following steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. On the Software Library Home page, from the **Actions** menu, click **Export** to export entities present in the Software Library as a Provisioning Archive (PAR) file.

The PAR file can be used for recreating the entities on an Enterprise Manager with a different repository.

3. On the Export Software Library Entities page, do the following:
 - Click **+Add** to search and select an entity.
 - In **Directory Location**, enter a directory location accessible to OMS for storing the generated PAR files.
 - In **PAR File**, enter the name of the PAR file with a `.par` extension generated during export.
 - To encrypt and securely store all the secret property values of the PAR file being exported, enter a value in the **Oracle Wallet Password** field.

Note: Specify the same password for importing this PAR file. For more information on importing, see [Importing Entities](#).

- Select **Exclude Associated Files**, to exclude the files, binaries, or scripts associated with an entity, from being exported.

For example, let us consider that you have a separate test and production environment and want to import only the entities that have been tested and certified in the test environment into production. The entities exported from the test system are made available as a Provisioning Archive (PAR) file. You can now choose to import this PAR file into the production system (which is identical to the test system) and use the tested entities.

4. Click **Submit** to submit an export job. Once the job runs successfully, the selected entities from the Software Library are exported as a PAR file.

① Note

Enterprise Manager does not support exporting Oracle-owned entities.

Importing Entities

To import PAR (Provisioning Archive) files into the Software Library or deploy them to an OMS, perform the following steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. On the Software Library Home page, from **Actions** menu, click **Import** to import the PAR files.
3. On the Import Software Library Entities page, specify the **PAR File** to be imported.

To import the PAR file successfully, in the **Password** field, enter the same password that was set on the PAR file to secure the secret property values during export.

For example, let us consider that you have a separate test and production environment and want to import only the entities that have been tested and certified in the test

environment into production. The entities exported from the test system are made available as a Provisioning Archive (PAR) file. You can now choose to import this PAR file into the production system (which is identical to the test system) and use the tested entities.

4. If a revision of the entity being imported already exists in Software Library, then you can overwrite the existing entity with a newer revision during import by selecting **Force New Revision**.

Note: If a revision of the entity being imported already exists in the repository, and you do not select the Force New Revision option, then import process fails.

5. Click **Submit** to submit an import job. On successful completion of the job, the PAR files are imported into the Software Library.

Staging Entities

For transferring files associated with multiple entities to multiple target hosts, follow the steps outlined in this section.

Prerequisites

Ensure that you meet the following prerequisites before staging the files:

1. Only hosts that are monitored by the Enterprise Manager can be specified as the destination for staging the files associated with an entity.
2. For each entity, only files that have been successfully uploaded to the entity (hence, in *Ready* status) can be selected for staging.

① Note

To verify if the entity has any files in the **Ready** state, follow these steps:

- a. Select the entity, and click **View**.
- b. On the View Entity page, select **Select Files** tab, to verify the files associated with the entity.
- c. Unless there is at least one file with a *Ready* status, you cannot proceed with the staging process.

3. Only users with View Job Privileges can perform staging.
4. Only entities for which the user has at least view privileges can be selected for staging.
5. The location should be writeable using the credential given for the target host.
6. If the source files to be staged are on NFS, then the credentials used for browsing the destination target should have `root` permissions to be able to mount the NFS location.

Staging Procedure

Log in to Enterprise Manager and perform the following steps:

1. From the **Enterprise** menu, select **Jobs and Procedures**, then select **Software Library**.
2. From the **Actions** menu, select **Stage Entities**.
3. On the Stage Entities page, expand the Entities section (if not already expanded).
4. Click **+Add** to search and select the entities. Only those entities which are not already added and those that have at least one file in the READY status can be added.

5. All the files in the READY status are selected for staging by default. To change the selection, expand the row of the added entity in the table and check/uncheck the Select column.
6. You can optionally select the Overwrite files on the staging location to overwrite an existing version of the same file. If not, ignore this option and proceed.
7. In the Staging Destination section, click **+Add** to add the stage destination details.
8. Click **+Add** to select the target hosts for staging.
9. Specify the Stage Location in the text box applicable for the host targets selected.
10. Choose the credentials that should be used for staging. If more than one host target is selected, then the stage location should be writeable using the selected credential on each host.
11. Click **OK** to update the selected hosts in the staging destination table.
12. Click **Submit**.
13. To verify the status of the submitted job, click the Job Details link that leads to the File Transfer Activity page displaying the file transfer details. Alternately, from the **Enterprise** menu, select **Job**, then click **Activity** and search for the job.

Maintaining Software Library

To maintain the health and proper functionality of the Software Library, the administrator who configured the Software Library, or the Designer who has administration access on it must perform the tasks listed here.

This section includes:

- [Periodic Maintenance Tasks](#)
- [Re-Importing Oracle Owned Entity Files](#)
- [Removing \(and Migrating\) Software Library Storage Location](#)
- [Removing a Referenced Storage Location](#)
- [Deactivating and Activating a Storage Location](#)
- [Scheduling Purge Job](#)
- [Backing Up Software Library](#)

Periodic Maintenance Tasks

Periodically, the Administrator must perform the following tasks for proper functioning of the Software Library:

- Refresh the Software Library regularly to compute the available space, free space, and the space used by deleted entities. To do so, on the Administration page, in the upload file locations tab, select the storage location. From the **Actions** menu, select **Refresh**. On successful refresh, a confirmation is displayed. Alternately, you can search for the periodic refresh job `SWLIBREFRESHLOCSTATS`, and edit the schedule and other attributes to suit your requirements. By default, this job is scheduled to run every 6 hours.
- Purge deleted entities to conserve disk space. To do so, see [Scheduling Purge Job](#). Alternatively, you can search for the periodic purge job `SWLIBPURGE`, and edit the schedule and attributes to suit your requirements. By default, this job is scheduled to run every 24 hours.

- Check accessibility of the configured Software Library locations. To do so, on the Administration page, in the upload file locations tab, select the storage location. From the **Actions** menu, select **Check Accessibility**.

Re-Importing Oracle Owned Entity Files

Note

Re-importing metadata applies only to the Oracle owned files, which means all the entity files offered with the Enterprise Manager product by default. The metadata of User owned entity files cannot be recovered through the Re-import functionality.

Re-Importing the metadata of Oracle owned entity files is not a periodic activity. Re-import helps to recover the metadata files in one of the following situations:

- If you delete the file system location where the metadata was imported. For example, /scratch/swlib1/
- If the import job submitted while creating the first upload location fails.

To re-import the metadata of Oracle owned files, do the following:

1. In Enterprise Manager, from **Setup** menu, select **Provisioning and Patching**, and then click **Software Library**.
2. On the Software Library Administration page, in the Upload File Location tab, from **Actions** menu, select **Re-Import Metadata** option to submit a job that re-initiates the re-import process.

Removing (and Migrating) Software Library Storage Location

Software Library Storage Administrators have the required privileges to delete a storage location. If a storage location is not in use, then you can remove it instantly. However, if it is in use, then you must migrate the contents to another location so that the entities using these files continue to remain usable.

Before removing a storage location that is currently in use, you are prompted for an alternate location for the files. After you select an alternate location, a migration job is submitted, and the location is marked as **Migrating**. After successful migration of the entity files to the new location, the location configuration is deleted. In case of any errors during migration, the location is marked as **Inactive**. Once the errors are fixed, and the storage administrator ascertains that the location is good to use, the location is marked as **Active**.

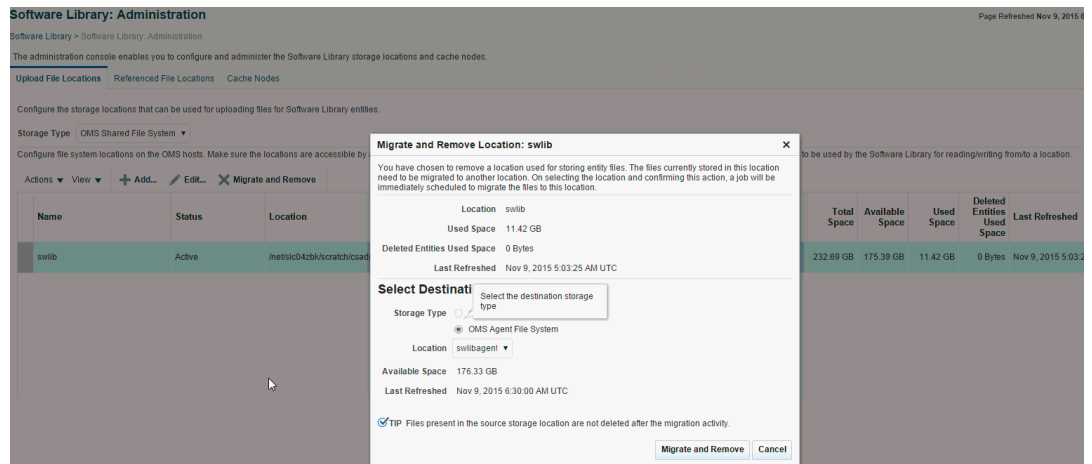
Note

To remove a location from OMS Agent File System or Referenced Agent File System storage, you must have a view privilege on the credentials for the location being removed, and the alternate location where the files are migrated.

To delete a configured storage location, perform the following steps:

1. In Enterprise Manager, from **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.

- On the Software Library Administration page, select the storage location, and click **Migrate and Remove**.



- On the Migrate and Remove Locations dialog box, select either **OMS Shared File System** or **OMS Agent File System**. A list of available active storage locations are displayed, select one and click **Migrate and Remove**.

Note

At least one upload location (either OMS Shared File System or OMS Agent File System) should be present. The last active upload location cannot be removed. Use the steps listed in the Enterprise Manager console or EMCLI to migrate an upload location to another upload location of either upload storage types (either OMS Shared File System or OMS Agent File System). For example, you can migrate an OMS Shared File System storage location to an OMS Agent File System storage location. Even the reverse operation is supported. However, note that this type of migration, across storage types, is supported specifically for *upload* storage types, and is not applicable for the reference storage types.

For a storage location, if there are no active upload locations (OMS Shared File System or OMS Agent File System), then the **Migrate and Remove** button will not be enabled for that location.

To migrate the files from one upload location to another, you can also use the EM CLI verb `emcli remove_swlib_storage_location`. For more information about this command, see [Performing Software Library Tasks Using EM CLI Verbs or in Graphical Mode](#).

- In the confirmation dialog box, click **Migrate and Remove** to submit a job, which on successful completion deletes the storage entry from the table.

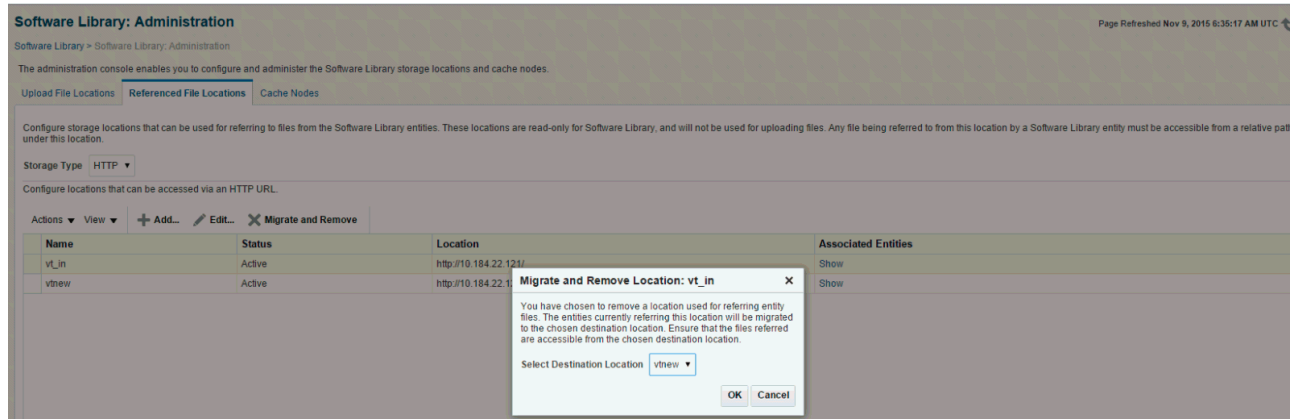
Note

When one storage location is migrated to another location, for example, from `/vol/swlib1` to `/vol/swlib2`, the file system contents of the source location (`/vol/swlib1`) are not deleted during the migration. However, going forward, the source location and the files are never referenced by Software Library.

Removing a Referenced Storage Location

To remove a configured reference storage location (HTTP/ NFS/ External Agent Location), perform the following steps:

1. In Enterprise Manager, from **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library Administration page, select the storage location, and click **Migrate and Remove**.



Note

If a location is not in use, then select the storage location and click **OK** to remove the location. However, if some entities are using a storage location, then you must migrate the files to another location before deleting the existing location.

3. To migrate the files to another location from the Migrate and Remove Locations dialog box, select a destination location from the list of active storage locations, then click **OK**.

Note

If there are no active locations of the same storage type available for migration, then the **Migrate and Remove** button is disabled for the location.

Deactivating and Activating a Storage Location

An upload or reference storage location can be deactivated. Once deactivated, the status of the storage location becomes **Inactive** and no further uploads will be allowed to the upload storage location. A storage location in an inactive state can be activated to be put back in use.

To deactivate a storage location, follow these steps:

1. In Enterprise Manager, from **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.

2. On the Software Library Administration page, select the storage location that is in an **Active** state, then from the **Actions** menu select **Deactivate**. A confirmation dialog is displayed.
3. Upon confirmation, the storage location is deactivated, and state changes to **Inactive**.

To activate a storage location, follow these steps:

1. In Enterprise Manager, from **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library Administration page, select the storage location that is in an inactive state, then from the **Actions** menu select **Activate**. A confirmation dialog is displayed.
3. Upon confirmation, the storage location is activated, and state changes to **Active**.

Scheduling Purge Job

1. In Enterprise Manager, from **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library Administration page, select the storage location, and from the Actions menu select **Purge**. The following dialog box appears where you can schedule the purge job:

Purge Deleted Entities Files

Enter the schedule for the purge job. This job will purge the files of deleted entities from all configured OMS Shared File System locations.

Start ☒ Immediately ☐ Later (UTC-08:00) Los Angeles - Pacific Time (PT)

Repeat Do not repeat

Grace Period ☐ Do not run if it cannot start within 1 hours of the scheduled start time

Duration ☒ Indefinitely ☐ For 1 hours Until

OK Cancel

3. Enter all the details and click **OK** to submit the job, on successful completion of the job all the deleted entities are removed from the storage location.

However, you can also perform this operation in the following method:

1. In Enterprise Manager, from **Setup** menu, select **Provisioning and Patching**, then select **Software Library**.
2. On the Software Library Administration page, from the Actions menu, select Deleted Entities. The list of deleted entities with type, subtype, owner, and size is displayed.
3. Click **Purge** to submit the job, on successful completion of the job all the deleted entities are removed from the storage location.

Backing Up Software Library

For information about backing up your Software Library, see the chapter on "Backing Up and Recovering Enterprise Manager" in the Enterprise Manager Advanced Installation and Configuration Guide.

4

Managing Plug-Ins

This chapter provides an overview of Plug-In Manager, and describes how you can use it to view, deploy, administer, and undeploy plug-ins.

In particular, this chapter covers the following:

- [Introduction to Plug-ins](#)
- [Workflow of Plug-In Deployment](#)
- [Introduction to Plug-In Manager](#)
- [Knowing Your Plug-Ins](#)
- [Downloading, Deploying, and Upgrading Plug-Ins](#)
- [Undeploying Plug-Ins](#)
- [Advanced Operations with Plug-Ins](#)
- [Troubleshooting](#)

Note

In a new release, some plug-ins may be obsoleted while some may be deprecated. Obsoleted plug-ins will not be supported on Enterprise Manager completely, whereas deprecated plug-ins will not be supported from future releases. When upgrading to a new release version, the obsoleted plug-ins need to be undeployed from Enterprise Manager. For details, see [Obsolete and Deprecated Plug-ins](#).

Getting Started

[Table 4-1](#) provides a quick view of the sections within this chapter that might be of interest to you.

Table 4-1 Getting Started

User	Sections of Interest
Beginner	<ul style="list-style-type: none">• Introduction to Plug-ins• Workflow of Plug-In Deployment• Introduction to Plug-In Manager
Basic	<ul style="list-style-type: none">• Workflow of Plug-In Deployment• Customizing Your View• Checking the Availability of Plug-Ins• Viewing Information about Plug-Ins

Table 4-1 (Cont.) Getting Started

User	Sections of Interest
Intermediate	<ul style="list-style-type: none"> • Customizing Your View • Checking the Availability of Plug-Ins • Viewing Information about Plug-Ins • Downloading Plug-Ins • Deploying Plug-Ins to Oracle Management Service (Reduce OMS Restart time and Downtime) • Upgrading Plug-Ins Deployed to Oracle Management Service • Deploying Plug-Ins on Oracle Management Agent • Upgrading Plug-Ins Deployed to Oracle Management Agent • Undeploying Plug-Ins from Oracle Management Service • Undeploying Plug-Ins from Oracle Management Agent • Troubleshooting
Advanced	<ul style="list-style-type: none"> • Re-deploying Plug-Ins on Oracle Management Agent • Deploying Plug-In Patches While Deploying or Upgrading Management Agent (Create Custom Plug-In Update) • Troubleshooting

Introduction to Plug-ins

This section covers the following:

- [Enterprise Manager Extensibility Paradigm](#)
- [Plug-Ins](#)
- [Plug-Ins Deployed by Default](#)
- [Plug-In Releases](#)
- [Roles Required to Manage Plug-Ins](#)

Enterprise Manager Extensibility Paradigm

Enterprise Manager is system management software that delivers centralized monitoring, administration, and life cycle management functionality for the complete IT infrastructure, including systems running Oracle and non-Oracle technologies.

Enterprise Manager has grown in size and magnitude over the years to offer a spectrum of powerful IT management and monitoring solutions. This growth has lead to changes in managing support for new features, enhancements, and bug fixes.

Considering these developments, Oracle has carefully redesigned the architecture of Enterprise Manager in such a way that the framework or the core base on which the product runs is clearly separated from the layer that offers IT solutions by means of features. This new architecture implemented in Enterprise Manager enables Oracle to provide a much stronger framework with capabilities to extend itself seamlessly from time to time for supporting new features and enhancements.

You no longer have to wait for the next release of Enterprise Manager to access the latest monitoring features for released products. The pluggable framework in Enterprise Manager allows target support to be included soon after new versions of targets ship. You can install a new Enterprise Manager system or upgrade an existing one, as soon as the Enterprise Manager release is made available by Oracle.

Based on the new design, Enterprise Manager has the following logical parts:

- **EM Platform:** Consists of a set of closely integrated UI and backend services that most monitoring and management functionality in Enterprise Manager depends on. Examples of platform subsystems include the Enterprise Manager target and metric model, the job, event, and provisioning framework. The platform also includes Oracle Management Agent (Management Agent) as well as the core background services such as the data loader, job dispatcher, and notification manager. The platform is delivered as part of an Enterprise Manager release, and can only be upgraded by upgrading to a new version of Enterprise Manager.
- **EM Plug-ins:** Modules that can be plugged to an existing Enterprise Manager Platform to provide target management or other vertical functionality in Enterprise Manager. Plug-ins offer special solutions or new features, for example, connectivity to My Oracle Support, and extend monitoring and management capability to Enterprise Manager, which enable you to monitor a particular target on a host. Plug-ins work in conjunction with OMS and Management Agent to offer monitoring services, and therefore they are deployed to the OMS as well as the Management Agent.

The plug-in releases happen more often than Enterprise Manager Core Platform releases. The plug-ins enable Enterprise Manager to be updated with new features and management support for the latest Oracle product releases, without having to wait for the next platform release to provide such functionality.

Plug-Ins

Plug-ins are modules that can be plugged into an existing Enterprise Manager deployment to extend target management or other vertical functionality in Enterprise Manager.

At a high level, plug-ins contain archives for monitoring and discovering OMS instances and Management Agents. The archives contain Java and SQL codes, and metadata.

Plug-Ins Deployed by Default

As a part of Enterprise Manager installation, a set of basic plug-ins is deployed by default. You can deploy other plug-ins to extend the basic functionality of Enterprise Manager.

The plug-ins that are deployed by default, or are shipped out of box are as follows.

- Oracle Database: `oracle.sysman.db`
- Oracle Fusion Middleware: `oracle.sysman.emas`
- Oracle Systems Infrastructure: `oracle.sysman.si`
- Oracle Exadata: `oracle.sysman.xa`
- Oracle Cloud Framework: `oracle.sysman.cfw`

Plug-In Releases

Plug-in releases happen more often than Enterprise Manager Core platform releases. This new pluggable framework enables Enterprise Manager to be updated with management support for the latest Oracle product releases, without having to wait for the next platform release to provide such functionality.

For example, when a new version of Oracle Database is released, you can simply download and deploy the latest Oracle Database plug-in, which will include management support for the latest Oracle Database release. You can also work with plug-ins in Offline Mode.

Obsolete and Deprecated Plug-ins

Obsolete plug-ins are plug-ins that are not supported for the current and future releases of Enterprise Manager. These plug-ins must be undeployed from the Management Agents and Oracle Management Services before upgrading to a new Enterprise Manager release.

Deprecated plug-ins are plug-ins for which support will not be available in the future releases of Enterprise Manager. Oracle recommends you limit your deployment of the deprecated plug-ins.

To undeploy obsolete and deprecated plug-ins from Enterprise Manager, first undeploy the plug-ins from the Management Agent (see [Undeploying Plug-Ins from Oracle Management Agent](#)), and then from the OMS (see [Undeploying Plug-Ins from Oracle Management Service](#)).

It is recommended that you remove the plug-in binaries of the undeployed plug-ins from Self Update.

Roles Required to Manage Plug-Ins

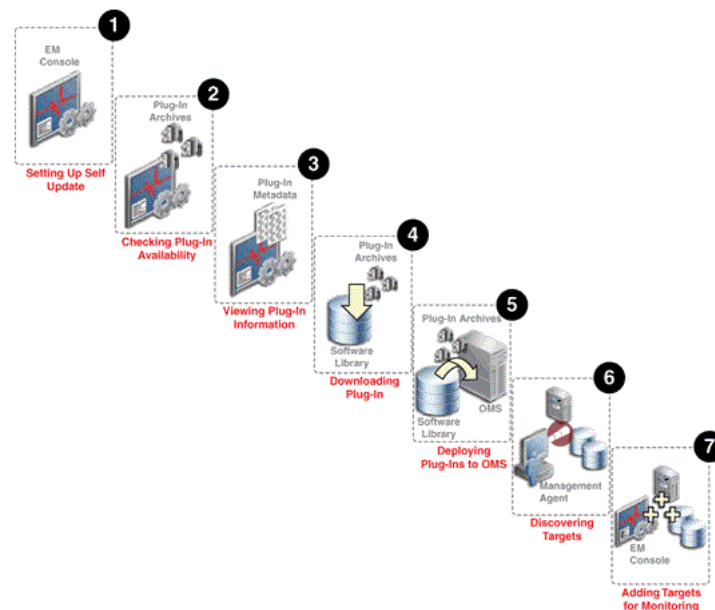
You need one or more of the following out-of-the-box roles to download, manage, and deploy plug-ins:

- EM_PLUGIN_OMS_ADMIN: Enables you to manage the lifecycle of plug-ins on Management Server instances.
- EM_PLUGIN_AGENT_ADMIN: Enables you to manage the lifecycle of plug-ins on Management Agents.
- EM_PLUGIN_USER: Enables you to view the plug-in lifecycle console.

Workflow of Plug-In Deployment

[Figure 4-1](#) illustrates the workflow of plug-in deployment—how you typically set up the Enterprise Manager infrastructure, deploy plug-ins to OMS, and discovery and monitor targets using the deployed plug-ins.

Figure 4-1 Plug-In Deployment Workflow



Step 1: Setting up Self-Update Console

Self Update console is a common dashboard used for reviewing, downloading, and applying new updates available for Enterprise Manager. The console frees you from having to monitor multiple channels to get informed about new updates that are available from Oracle. The updates automatically downloaded by Self Update include plug-ins. For checking the availability of plug-ins and downloading them to Enterprise Manager, you must set up the Self Update Console. Set up the Self Update Console as described in [Updating Enterprise Manager](#).

Step 2: Checking Plug-In Availability

Checking the plug-in availability essentially refers to the act of verifying whether the plug-ins are available on My Oracle Support for download and deployment in Enterprise Manager. This is a prerequisite before downloading plug-ins. To check plug-in availability, follow the steps outlined in [Checking the Availability of Plug-Ins](#).

Step 3: Viewing Plug-In Information

Viewing plug-in information refers to the act of viewing basic information related to a particular plug-in, such as the plug-in ID, the plug-in release number, and other basic information. You must view plug-in information to understand what targets and operating systems are certified for plug-ins. You can also check whether or not a particular plug-in has already been deployed. To view plug-in information, follow the steps outlined in [Viewing Information about Plug-Ins](#).

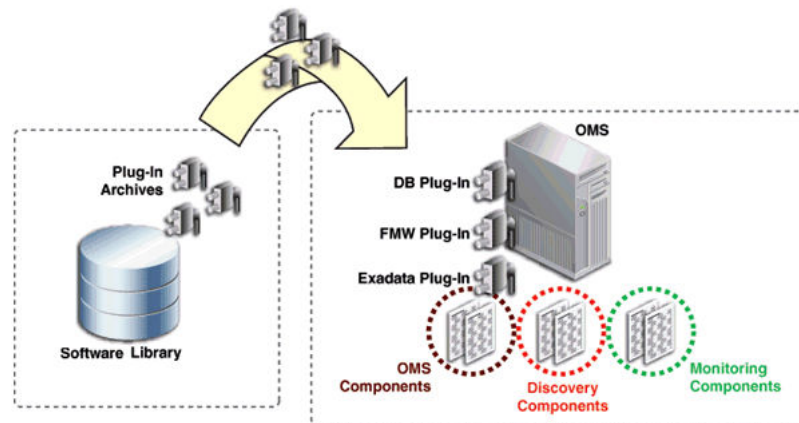
Step 4: Downloading Plug-Ins

Downloading plug-ins is the act of downloading plug-in archives or components, and its metadata, from My Oracle Support to Oracle Software Library (Software Library), so that they can be deployed suitably for discovering and monitoring certain targets. If you find that a particular target is not being monitored by plug-ins, you must download the required plug-ins. You can download both in online mode and offline mode. To download plug-ins, follow the steps outlined in [Downloading Plug-Ins](#).

Step 5: Deploying Plug-Ins to OMS

Deploying plug-ins to OMS is the next natural course of action once a plug-in is downloaded from My Oracle Support. This is to ensure the OMS capabilities are extended to either manage a new target or to add a new vertical capability. The installation and configuration of plug-ins on the OMS is essentially referred to as *Deployment*. Some plug-ins, when deployed, require the OMS to be re-started.

[Figure 4-2](#) illustrates how plug-ins are deployed to the OMS.

Figure 4-2 Deploying Plug-Ins to OMS

When the plug-in archives are deployed from the Software Library to the OMS, the OMS receives three different components for each plug-in, namely the OMS plug-in components, the discovery plug-in components, and the monitoring plug-in components.

Discovery plug-in components are those components that help in the discovery of unmanaged targets. Monitoring plug-in components are those components that help in the adding of discovered targets to Enterprise Manager console for monitoring purposes.

To deploy plug-ins on OMS, follow the steps outlined in [Deploying Plug-Ins to Oracle Management Service \(Reduce OMS Restart time and Downtime\)](#).

Step 6: Discovering Targets

Discovering targets refers to the process of identifying unmanaged hosts and targets in your environment. During discovery of targets, the discovery components of plug-ins are deployed to the Management Agent home. Note that this enables Enterprise Manager to only identify a new target in your environment; it however does not monitor the target.

After converting unmanaged hosts to managed hosts in Enterprise Manager, you must configure automatic discovery of targets on those hosts so that the unmanaged targets running on those hosts can be identified.

For instructions to configure automatic discovery of targets on managed hosts, refer to Discovery in the *Oracle Enterprise Manager Monitoring Guide*.

Note

When you configure automatic discovery of targets on managed hosts, discovery plug-in components are copied to Management Agent.

Once you have configured automatic discovery of targets on managed hosts, you must regularly check for discovered targets so that they can be promoted and monitored in Enterprise Manager.

For instructions to check for and promote discovered targets to managed status, refer to Discovery in the *Oracle Enterprise Manager Monitoring Guide*.

Note

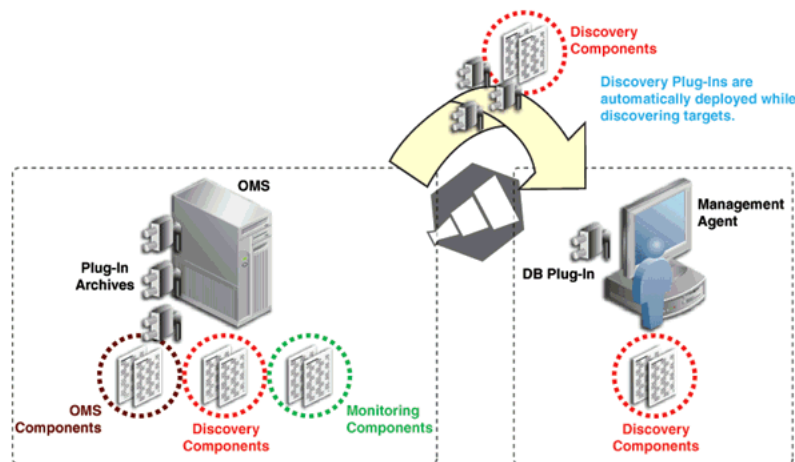
The plug-in for a specific target type is automatically deployed to the Management Agent that will monitor targets of that type. For example, if you discover a database target, the discovery plug-in component of the database plug-in is automatically deployed to the Management Agent installed on the database host.

However, this is true only for initial deployment. All subsequent updates to the Management Agent plug-in must be explicitly deployed. For example, if you want to deploy a new version of the database plug-in on the Management Agent, you must initiate the deployment using the instructions outlined in *Oracle Enterprise Manager Basic Installation Guide*.

Similarly, any patches to be applied on the Management Agent (framework or plug-in) must be explicitly applied using the instructions outlined in [Patching Oracle Management Agents](#).

[Figure 4-3](#) illustrates how the discovery plug-in components are deployed to the Management Agent while discovering new targets.

Figure 4-3 Discovering Targets

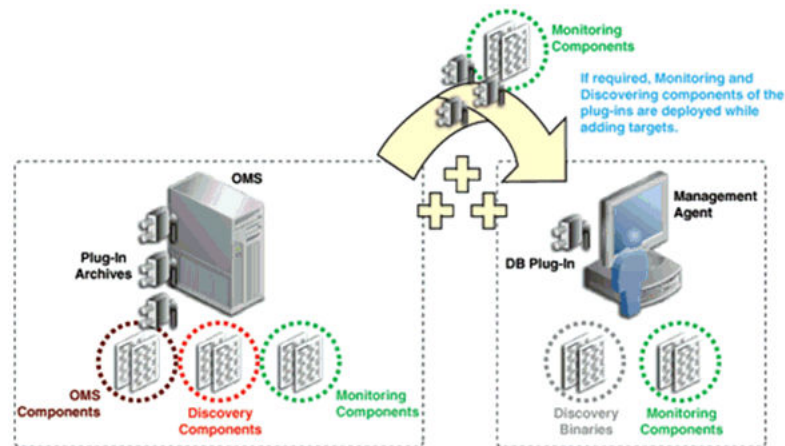


Step 7: Adding Targets for Monitoring

Once the targets are discovered, they are added to the infrastructure, so that they can be monitored in Enterprise Manager. While adding targets, the monitoring components of plug-ins are deployed to the Management Agent home.

[Figure 4-4](#) illustrates how the monitoring plug-in components are deployed to the Management Agent while adding targets.

Figure 4-4 Adding Targets



Introduction to Plug-In Manager

Plug-In Manager is a feature of Enterprise Manager that serves as a single window solution for performing all plug-in deployment-related activities, through GUI as well as CLI. Using Plug-In Manager, you can:

- View plug-ins available for download; plug-ins that have been downloaded; and plug-ins that have been deployed to Enterprise Manager.
- View certification and critical information about plug-ins such as the name of the plug-in, the vendor who supplied it, the plug-in ID and version, and a short description.
- Deploy plug-ins on OMS.
- Deploy and re-deploy plug-in on Management Agent.
- Create custom plug-in update.
- Undeploy plug-ins from OMS and Management Agent.
- View the status of a plug-in deployment operations.

Accessing Plug-In Manager

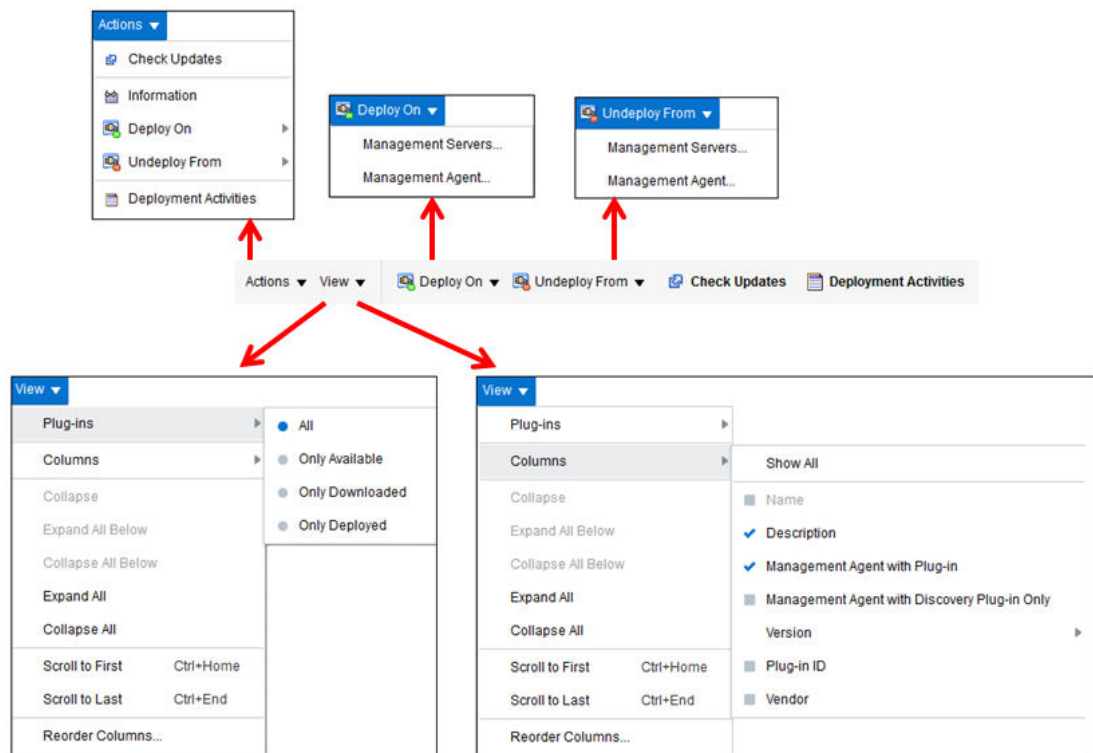
To access the Plug-In Manager console, from the **Setup** menu, select **Extensibility**, and then select **Plug-ins**.

Performing Operations Using Plug-In Manager

Using Plug-in Manager, you can deploy, upgrade, redeploy, and undeploy plug-ins.

[Figure 4-5](#) shows the operations you can perform using the Plug-In Manager.

Figure 4-5 Plug-In Manager Operations



Knowing Your Plug-Ins

This section explains the following:

- [Customizing Your View](#)
- [Checking the Availability of Plug-Ins](#)
- [Viewing Information about Plug-Ins](#)

Customizing Your View

This section tells you how to customize your view, and organize the plug-ins and columns displayed.

Customizing Displayed Plug-Ins

Over a period of time, as you download and deploy plug-ins, the number of plug-ins on your list increases. You can sort these plug-ins to view only the ones you require, for example, only the plug-ins available, or only the plug-ins deployed.

In order to customize your view, follow these steps.

1. From the **View** menu, select **Plug-Ins**.
2. From the Plug-Ins menu, select one of the following filters.
 - **All**, using this filter, you can view all plug-ins, including available, downloaded, and deployed plug-ins.

- **Only Available**, using this filter, you can view the plug-ins that are available for download.
- **Only Downloaded**, using this filter, you can view the plug-ins that are downloaded.
- **Only Deployed**, using this filter, you can view the plug-ins that are deployed.

Customizing Displayed Columns

By default, only a few columns of information are displayed. Optionally, you can either enable other columns of your interest, or disable ones that are already displayed.

In order to customize the displayed columns, follow these steps.

1. From the **View** menu, select **Columns**.
2. From the Columns menu, select one of the following filters for columns.
 - **Show All**, using this filter, you can view all columns.
 - **Vendor**, using this filter, you can view information about the vendor.
 - **Plug-In Id**, using this filter, you can view the plug-in id.
 - **Version**, this filter has three options you can choose from. They are as follows.
 - **Latest Available**, using this filter, you can view the newest plug-ins that are available.
 - **Latest Downloaded**, using this filter, you can view the plug-ins that have been downloaded recently.
 - **On Management Server**, using this filter, you can view the plug-ins that are deployed to the OMS.
 - **Management Agent with Discovery Plug-Ins Only**, this filter displays the Management Agent which has only Discovery Plug-Ins deployed.
 - **Management Agent with Plug-In**, this filter displays the Management Agent which has any plug-in deployed on it.
 - **Description**, this filter displays the description of the plug-ins.

Checking the Availability of Plug-Ins

To check the availability of plug-ins, follow these steps:

1. Set up the Self Update console as described in [Setting Up Self Update](#).
2. From the **Setup** menu, select **Extensibility**, then select **Plug-ins**.
3. On the Plug-ins page, in the Latest Available column of the table, check whether the plug-ins are available.

To refresh the list of available plug-ins, click **Check Updates**. Note that clicking Check Updates will take you to the Self Update page.

Viewing Information about Plug-Ins

This section gives you more information on plug-ins, and functions related to plug-ins. This section covers the following sections:

- [Differentiating Plug-In Releases from Enterprise Manager Platform Releases](#)
- [Identifying Plug-In ID](#)

- [Viewing Targets and Operating Systems Certified for Deployed Plug-Ins](#)
- [Viewing Plug-In Dependencies](#)
- [Verifying Deployed Plug-Ins](#)

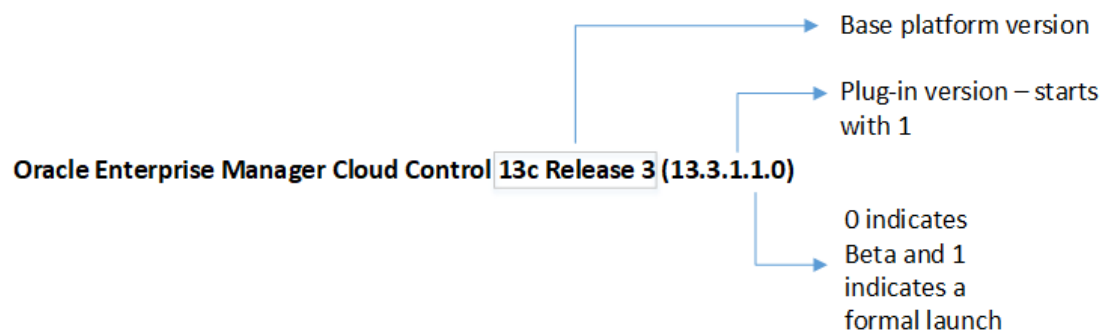
Differentiating Plug-In Releases from Enterprise Manager Platform Releases

Plug-ins have independent release cycles and release numbers, which may or may not be tied to Enterprise Manager product releases and release numbers.

Plug-in releases typically happen more often than Enterprise Manager platform releases.

[Figure 4-6](#) describes how plug-in releases are numbered.

Figure 4-6 Plug-In Release Number Format



[Figure 4-7](#) describes how Enterprise Manager platform releases are numbered.

Figure 4-7 Enterprise Manager Core Platform Release Number Format



Note

For Enterprise Manager platform releases where there was no beta, the beta/production value would always be zero. For example, the release version would be 13.3.0.0.0 and not 13.3.0.1.0.

Identifying Plug-In ID

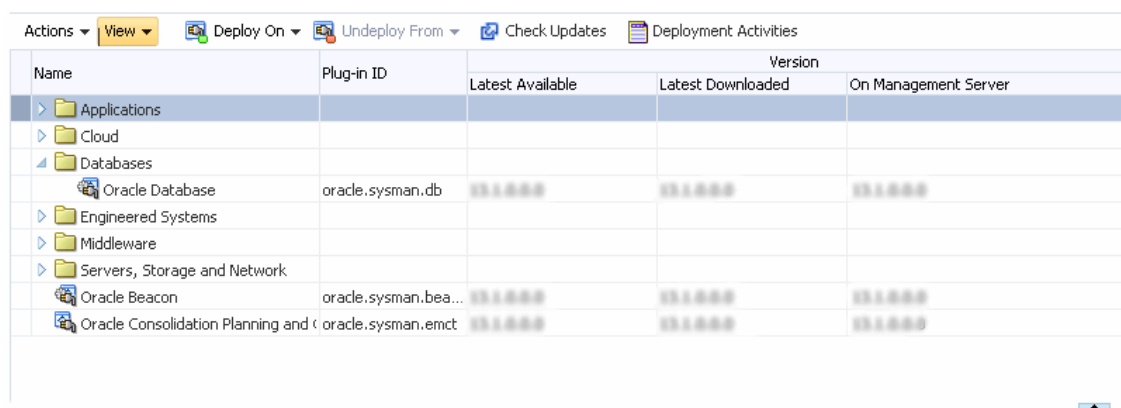
To identify the ID of a plug-in, follow these steps:

1. From the **Setup** menu, select **Extensibility**, then select **Plug-ins**.
2. On the Plug-ins page, in the Plug-in ID column of the table, note the plug-in ID of the plug-in of your interest.

If you do not see this column, from the **View** menu, select **Columns**, then select **Plug-in ID**.

[Figure 4-8](#) illustrates how you can identify the plug-in ID of the Oracle Database plug-in.

Figure 4-8 Identifying Plug-In ID



Name	Plug-in ID	Latest Available	Latest Downloaded	On Management Server
Applications				
Cloud				
Databases				
Oracle Database	oracle.sysman.db	19.1.0.0.0	19.1.0.0.0	19.1.0.0.0
Engineered Systems				
Middleware				
Servers, Storage and Network				
Oracle Beacon	oracle.sysman.bea...	19.1.0.0.0	19.1.0.0.0	19.1.0.0.0
Oracle Consolidation Planning and	oracle.sysman.emct	19.1.0.0.0	19.1.0.0.0	19.1.0.0.0

Viewing Targets and Operating Systems Certified for Deployed Plug-Ins

To view a list of targets and operating systems certified for a deployed plug-in, follow these steps:

1. From the **Setup** menu, select **Extensibility**, then select **Plug-ins**.
2. On the Plug-ins page, select the plug-in of your interest, and from the **Actions** menu, select **Information**.
3. On the Plug-in Information page, in the **General** tab, review the information provided in the **Certified Targets** and **Certified Operating Systems** tables.

Viewing Plug-In Dependencies

To view the dependencies of the preferred plug-in, follow these steps:

1. From the **Setup** menu, select **Extensibility**, then select **Plug-ins**.
2. On the Plug-ins page, select the plug-in of your interest, and from the **Actions** menu, select **Information**.
3. On the Plug-in Information page, in the **Dependencies** tab, review the information provided in the tables.

Verifying Deployed Plug-Ins

To view and administer the deployed plug-ins, from the **Setup** menu, select **Extensibility**, then select **Plug-ins**. Enterprise Manager displays the Plug-ins page, which is essentially the *Plug-In Manager* console.

To identify the OMS instances on which the plug-in of your interest is deployed, follow these steps using Enterprise Manager console:

1. From the **Setup** menu, select **Extensibility**, then select **Plug-ins**.
2. On the Plug-ins page, select the plug-in of your interest, and from the **Actions** menu, select **Information**.
3. On the Plug-in Information page, in the **Management Servers** tab, review the Oracle Management Services on which the plug-in is deployed.

To identify the Management Agents on which the plug-in of your interest is deployed, follow these steps using Enterprise Manager console:

1. From the **Setup** menu, select **Extensibility**, then select **Plug-ins**.
2. On the Plug-ins page, select the plug-in of your interest, and from the **Actions** menu, select **Information**.
3. On the Plug-in Information page, in the **Management Agent** tab, review the Management Agents on which the plug-in is deployed.

Example 4-1 Sample List of Plug-Ins Deployed on OMS

example.com:7654_Management_Service

Plug-in Name	Plug-in ID	Version (Revision)
Oracle Database	oracle.sysman.db	24.1.1.0.0
Oracle Fusion Middleware	oracle.sysman.emas	24.1.1.0.0
Oracle Exadata	oracle.sysman.xa	24.1.1.0.0
Oracle Cloud Application	oracle.sysman.ssa	24.1.1.0.0

Example 4-2 Sample List of Plug-ins Deployed on Management Agent

```
emcli list_plugins_on_agent -agent_names=agent1.example.com:3872
Lists plug-ins on the agent agent1.example.com
```

```
emcli list_plugins_on_agent -agent_names=agent1.example.com:3872,agent2.example.com:3872
-include_discovery
Lists plug-ins on both the agents provided along with their discovery components
```

```
emcli list_plugins_on_agent -agent_names='agent*,st*93'
Lists plug-ins on all agents with name matching one of the regular expressions agent* or st*93
```

```
emcli list_plugins_on_agent -all
Lists plug-ins on all the management agents.
```

To identify the Plug-ins deployed on OMS, on EM CLI, log in to EMCLI, and enter the following command. The command displays a list of all the plug-ins deployed on the OMS.

```
$emcli login
```

```
-username=<EM Console Username>  
[-password=<EM Console Password>]  
[-force]
```

```
$emcli list_plugins_on_server
```

To identify and view all the Plug-ins deployed on Management Agent, on EM CLI, enter the following command:

```
$emcli list_plugins_on_agent  
[agent_names="agent1,agent2,agent3..."  
[-all] [-include_discovery]
```

Downloading, Deploying, and Upgrading Plug-Ins

This section explains the following:

- [Downloading Plug-Ins](#)
- [Deploying Plug-Ins to Oracle Management Service \(Reduce OMS Restart time and Downtime\)](#)
- [Upgrading Plug-Ins Deployed to Oracle Management Service](#)
- [Deploying Plug-Ins on Oracle Management Agent](#)
- [Upgrading Plug-Ins Deployed to Oracle Management Agent](#)

Downloading Plug-Ins

You can download the plug-ins in online or offline mode. Online refers to an environment where you have Internet connectivity to the Enterprise Manager Store. Offline refers to an environment where you do not have Internet connectivity. This section contains the following sections:

- [Downloading Plug-Ins in Online Mode](#)
- [Downloading Plug-Ins in Offline Mode](#)
- [Importing Catalog Archives](#)
- [Importing Plug-In Archives](#)

Downloading Plug-Ins in Online Mode

To download the plug-ins in online mode, follow these steps:

1. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
2. On the Self Update page, in the table, click on **Plug-in**.
3. On the Plug-in Updates page, select the plug-in available for download, and click **Download**.

Multiple selection of plug-ins is not supported.

4. In the Schedule Download dialog, select an appropriate option to schedule the download. You can also select **Immediately** which schedules the job for immediate action. Select **Notify Once downloaded** if you want to be informed once the download is complete.

5. Click **Select**.

Enterprise Manager submits a job to download the selected plug-in from the Enterprise Manager Store to the Software Library.

A confirmation dialog appears to confirm that the job has been submitted successfully. In this confirmation dialog, you can click **Job Details** to track the status of the job.

Downloading Plug-Ins in Offline Mode

To download the plug-ins in offline mode, follow these steps:

1. Set Enterprise Manager to Offline Mode. To do so, follow these steps.
 - a. From the **Setup** menu, select **Provisioning and Patching**, then select **Offline Patching**.
 - b. In the Online and Offline Settings tab, select **Offline**.
2. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
3. On the Self Update page, click **Check for Updates**.

A message appears with the following URL to an Oracle site from where the updates catalog file can be downloaded.

https://updates.oracle.com/Orion/Download/download_patch/p9348486_112000_Generic.zip

4. From an Internet-enabled computer, download the catalog file using the aforementioned URL.
 5. Copy the downloaded catalog file to the OMS host or the Management Agent host where you plan to deploy the plug-ins.
 6. Import the catalog file to Enterprise Manager. For instructions, refer to [Importing Catalog Archives](#).
 7. On the Self Update page, in the table, click **Plug-in**.
 8. On the Plug-in Updates page, select the imported update that is available for download. Click **Download**.
- A message appears with a URL to an Oracle site from where the update can be downloaded.
9. From a computer that is connected to the internet, download the update using the aforementioned URL.
 10. Copy the downloaded file to the OMS host or the Management Agent host where you plan to deploy the plug-ins.
 11. Import the downloaded plug-in archive to Enterprise Manager. For instructions, refer to [Importing Plug-In Archives](#).

Importing Catalog Archives

To import a catalog archive, follow these steps:

1. Download the catalog archive as described in [Downloading Plug-Ins in Offline Mode](#).
2. Execute the following `emcli` command to import the downloaded catalog archive.

Example 4-3 Sample for Importing Catalog Archive

```
$emcli import_update_catalog
  -file="/u01/common/p9348486_112000_Generic.zip"
  -omslocal
```

Imports the master catalog file p9348486_112000_Generic.zip. The file must exist on the OMS host. In a multiple OMS setup, the request can be processed by any OMS, so the file should be accessible from the OMS processing the request. This means that the file must be kept on a shared location that is accessible from all the OMS instances.

```
$emcli import_update_catalog
  -file="/u01/common/p9348486_112000_Generic.zip"
  -host="host1.example.com"
  -credential_set_name="HostCredsNormal"
```

Imports the master catalog file p9348486_112000_Generic.zip that is present on the host host1.example.com. The host must be a managed host target in Enterprise Manager, and the Management Agent on this host must be up and running. The preferred unprivileged credentials for host host1.example.com are used to retrieve the remote file.

```
$emcli import_update_catalog
```

```
-file="file"
```

```
-omslocal
```

```
emcli import_update_catalog
```

```
-file="file"
```

```
-host="hostname"
```

```
[-credential_set_name="setname"] | -credential_name="name" -
credential_owner="owner"
```

Importing Plug-In Archives

Import plug-in archives to Oracle Software Library in the following cases:

- When you want to deploy any non-Oracle plug-ins, that is, plug-ins that have been created by a company other than Oracle, and are not available for download on the Self Update console.
- When you want to import other types of entity archives when Self Update is used in offline mode.

To import a plug-in archive, follow these steps:

1. Download the external archive as described in the previous section.
2. Set up the Enterprise Manager Command Line (EM CLI) utility. To do so, from the **Setup** menu, click **Command Line Interface**. Follow the instructions outlined on the Enterprise Manager Command Line Interface Download page.
3. Import the external archive in one of the following ways, depending on where EMCLI is installed.
 - If Enterprise Manager server is on the system on which you downloaded the plug-in archive (*.opar file), run the following command:

```
$emcli import_update
  -file="<path to *.opar file>"
  -omslocal
```

The `-omslocal` flag indicates that the plug-in archive path mentioned in the `-file` option is directly accessible to the EM server.

- If Enterprise Manager server is on a different system than the plug-in archive, run the following command:

```
$emcli import_update  
-file="<path to *.opar file you created>"  
-host="host1.example.com"  
-credential_name="host1_creds"  
-credential_owner="admin1"
```

The command syntax is as follows:

`-file`: The absolute path to the `*.opar` file on the system where you created the archive.

`-host`: The target name for a host target where the file is available.

`-credential_name`: The name of the credentials on the remote system you are connecting to.

`-credential_owner`: The owner of the credentials on the host system you are connecting to.

Note

As an alternative to the previous step, you can also run the following command:

```
$emcli import_update  
-file="<path to *.opar file you created>"  
-host="hostname"  
-credential_set_name="setname"
```

`-credential_set_name`: The set name of the preferred credential stored in the Management Repository for the host target. It can be one of the following:

- `HostCredsNormal`: The default unprivileged credential set.
- `HostCredsPriv`: The privileged credential set.

Deploying Plug-Ins to Oracle Management Service (Reduce OMS Restart time and Downtime)

You can deploy multiple plug-ins to an OMS instance in graphical interface or command line interface.

Note

- Plug-ins must be deployed on the OMS prior to being deployed on Management Agents.
- In a multi OMS environment, Plug-in Manager automates plug-in deployment on all the management servers.
- A plug-in upgrade failure could put the Management Repository in an inconsistent state. Oracle recommends that your repository database should be running in archive log mode, and that your backup policies are in place.
- The deployment time varies from one plug-in to another, depending on the volume of data populated in the Management Repository. A page is displayed that allows you to monitor the deployment status, as described in [Tracking the Deployment Status of Plug-Ins on Oracle Management Service](#).
- The deployment of some plug-ins requires the OMS to be stopped, and then restarted. This process occurs automatically as part of the plug-in deployment process.
- While deploying plug-ins to the OMS, OMS plug-in components, discovery plug-in components, and monitoring plug-in components are deployed to the OMS.

To deploy plug-ins to the OMS in graphical mode, follow these steps:

1. From the **Setup** menu, select **Extensibility**, then select **Plug-ins**.
2. On the Plug-ins page, select the plug-in you want to deploy.

Note

Alternately, you can move to the next step and select the plug-ins after the next step.

3. From the **Deploy On** menu, select **Management Servers**.
4. In the Deploy Plug-ins on Management Servers: Plug-ins page, verify that the plug-in details on the lower portion of the screen are correct. Additionally, you can add more plug-ins by clicking **Add**.
5. Select the **Use Last Successful Prerequisite** check box to skip the prerequisite checks.
The check box is enabled only if the plug-in had successfully cleared the prerequisite checks within the last 24 hours and was not deployed.
6. Click **Next**.
7. In the **Deploy Plug-ins on Management Servers: Prerequisite Checks** page, wait for the prerequisite checks to complete (if not cleared already) and click **Next**.
8. In the **Deploy Plug-ins on Management Servers: Repository** page, specify the Management Repository SYS credentials. Click **Named** option to select the saved credentials or click **New** option to enter new credentials.

The newly entered credentials will be automatically saved for future deployments, after the deployment is successful.

Note

SYS is the default Management Repository admin user. If you are using SYS, select SYSDBA role.

Starting with Enterprise Manager 13c Release 5 Update 15 or higher, you can deploy plug-ins on OMS using a non-SYS user as the Management Repository admin user by following the below steps:

- a. Create a non-SYS admin user in the Management Repository using the `CreateLCMUser` utility. For example, you can create a non-SYS user named `SYSMAN_ADMIN`.

For more information and instructions about how to create a non-SYS user, see *Evaluate LCM User Creation in the Enterprise Manager Advanced Installation and Configuration Guide*.

- b. In the **Deploy Plug-ins on Management Servers: Repository** page, provide the Management Repository non-SYS admin user credentials from **step a**. Click **New** option to enter the non-SYS user credentials and select **Normal** under Role.

The below screenshot shows an example using a non-SYS admin user named `SYSMAN_ADMIN`.

9. Click **Next**.

10. The **Deploy Plug-ins on Management Servers: Review** page displays the OMSs and the statuses of the OMSs where the plug-ins will be deployed, and the plug-ins. Verify that all the details are correct and click **Deploy**.

To deploy plug-ins to the OMS in silent mode, follow these steps:

1. Log in to EMCLI as follows:

```
$ORACLE_HOME/bin/emcli login -username=sysman
```

2. Run the following command if the emcli client is an old version, and does not have all required verbs:

```
$ORACLE_HOME/bin/emcli sync
```

3. To deploy the plug-ins on the OMS, run the following command:

```
$emcli deploy_plugin_on_server  
-plugin="plug-in_id[:version]  
[-sys_password=<sys_password>]  
[-prereq_check]"
```

For example:

```
$emcli deploy_plugin_on_server -plugin=oracle.sysman.empa -  
sys_password=SYS_PASSWORD
```

Note

- SYS is the default Management Repository admin user.

Starting with Enterprise Manager 13c Release 5 Update 15 or higher, you can deploy plug-ins using a non-SYS user as the Management Repository admin user, if preferred. In this case, you need to provide the credentials of the non-SYS admin user using the arguments: `-dbUser` and `-dbPassword` when running the following command:

```
$emcli deploy_plugin_on_server  
-plugin="plug-in_id[:version]  
[-dbUser=<non-SYS_dbuser>]  
[-dbPassword=<non-SYS_dbuserpassword>  
[-prereq_check]"
```

For example:

```
$emcli deploy_plugin_on_server -plugin=oracle.sysman.empa -  
dbUser=SYSMAN_ADMIN -dbPassword=SYSMAN_ADMIN_PASSWORD
```

- For information on plug-in id, refer to [Identifying Plug-In ID](#).

Note

The procedure for plug-in deployment remains the same even in a multi-OMS environment. Enterprise Manager automatically detects whether it is a single-OMS or a multi-OMS environment and in case of a multi-OMS environment, Enterprise Manager automatically deploys the selected plug-in on all OMS instances.

If the plug-in deployment fails on a primary OMS, where the Administration Server is running, then you must first address the issue, and then resume the deployment or restore the system from backup. If however, the plug-in deployment fails on a non-primary OMS, identify the cause for the failure. If there is a fix or a workaround, fix the problem, and perform the same steps again. The system automatically detects which OMS instances do not have the plug-ins deployed, and deploys them on those servers.

If the problem persists, contact Oracle Support.

Tracking the Deployment Status of Plug-Ins on Oracle Management Service

This section describes the procedure of monitoring the deployment status of plug-ins that do not require down time as well as those that do require down time.

To monitor the status of deployment and undeployment operations of plug-ins that require down time, execute the following command:

```
emctl status oms -details
```

To monitor the status of deployment and undeployment operations for plug-ins that do not require down time, follow these steps:

1. From the **Setup** menu, select **Extensibility**, then select **Plug-ins**.
2. On the Plug-ins page, do one of the following:
 - From the **Actions** menu, select **Deployment Activities**.
 - Select a plug-in, and click the **Recent Deployment Activities** tab at the bottom of the page. Alternatively, you can also run the following command using EMCLI.

```
$emcli get_plugin_deployment_status -plugin_id=<plugin_id>
```

Upgrading Plug-Ins Deployed to Oracle Management Service

You can upgrade across plug-in versions, that is, from one plug-in version to another higher plug-in version or a revision of another higher plug-in version.

To upgrade across plug-in versions deployed to the OMS, follow these steps:

1. Check for the latest available versions and revisions in the Enterprise Manager Store as described in [Checking the Availability of Plug-Ins](#).
2. Download them as described in [Downloading Plug-Ins](#).
3. Deploy them to the OMS as described in [Deploying Plug-Ins to Oracle Management Service \(Reduce OMS Restart time and Downtime\)](#).

Deploying Plug-Ins on Oracle Management Agent

While installing a Management Agent using the Add Host Targets Wizard, all the core discovery plug-ins available on the OMS are automatically deployed to the Management Agent.

For information about discovery plug-ins, refer to [Viewing Information about Plug-Ins](#).

If you want to deploy any additional plug-ins after installing the Management Agent, then follow these steps:

1. Set up the Self Update console.
2. Check whether the plug-ins are available on Enterprise Manager store. For instructions refer to [Checking the Availability of Plug-Ins](#).
3. Download the available plug-ins. For instructions, refer to [Downloading Plug-Ins](#).
4. Deploy the downloaded plug-ins to the Management Agent.
 - a. From the **Setup** menu, select **Extensibility**, then select **Plug-ins**.
 - b. On the Plug-ins page, select the plug-in you want to deploy.

- c. From the **Deploy On** menu, select **Management Agent**.
- d. Follow the steps mentioned in the Deploy Plug-ins on Management Agent dialogue box.
- e. Click **Deploy**.

To deploy plug-ins in EM CLI, use the following command:

```
$emcli deploy_plugin_on_agent  
  
-agent_names="agent1[:agent2...]"  
  
-plugin="plug-in_id[:version]"  
  
[-discovery_only]
```

To deploy the latest revision of the plug-in, run the command above with an additional argument: `allow_revision_update`.

Tracking the Deployment Status of Plug-Ins on Oracle Management Agent

To track the deployment status of plug-ins on Management Agent, refer to [Tracking the Deployment Status of Plug-Ins on Oracle Management Service](#).

Upgrading Plug-Ins Deployed to Oracle Management Agent

You can upgrade across plug-in versions, that is, from one plug-in version to another, higher plug-in version or a revision of another, higher plug-in version.

Note

You will upgrade the plug-in versions and revisions only on Management Agents that are already installed in your environment.

When a plug-in is deployed explicitly or a target is promoted on new Management Agents, then the latest plug-in version and revision automatically gets included from the OMS.

To upgrade across plug-in versions deployed to the Management Agent, follow these steps:

1. Check for the latest available versions and revisions in the Enterprise Manager Store as described in [Checking the Availability of Plug-Ins](#).
2. Download them as described in [Downloading Plug-Ins](#).
3. From the **Setup** menu, select **Extensibility**, then select **Plug-ins**.
4. On the Plug-ins page, select the plug-in you want to upgrade.
5. From the **Deploy On** menu, select **Management Agent**.
6. In the Deploy Plug-in on Management Agent dialog, select the version or revision of the plug-in you want to upgrade to., and click **Continue**.
7. Select the preferred Management Agent to upgrade the plug-in on, and click **Continue**. Then click **Next**. And then click **Deploy**.
8. On the Confirmation dialog, click **Close**.

Undeploying Plug-Ins

This section explains the following:

- [Undeploying Plug-Ins from Oracle Management Service](#)
- [Undeploying Plug-Ins from Oracle Management Agent](#)

Undeploying Plug-Ins from Oracle Management Service

To undeploy plug-ins from the OMS, follow the steps:

1. First, undeploy all plug-ins from all Management Agents. To do so, follow the steps mentioned in [Undeploying Plug-Ins from Oracle Management Agent](#).
2. From the **Setup** menu, select **Extensibility**, then select **Plug-ins**.
3. On the Plug-ins page, select the plug-in you want to undeploy, and from the **Actions** menu, select **Undeploy From**, then select **Management Servers**.
4. In the **Undeploy Plug-in From Management Server** dialog, enter the Management Repository admin user and password, click **Continue**, and then click **Undeploy**.

SYS is the default Management Repository admin user.

Note

Starting with Enterprise Manager 13c Release 5 Update 15 or higher, you can undeploy plug-ins using a non-SYS user as the Management Repository admin user, if preferred. In this case, you need to enter the credentials of the non-SYS admin user.

The below screenshot shows an example using a non-SYS admin user named SYSMAN_ADMIN.

Undeploy Plug-in From Management Server

General

Name: Oracle Audit Vault and Database Firewall

Version: 13.5.1.0.0

* Repository Admin User (For example: SYS or ADMIN):

* Repository Admin Password:

Repository admin user to undeploy the repository side artifacts of the plug-in

Target Types

Name	Supported Target Versions
Audit Vault Agent	12.2.0.0.0
Database Firewall	12.2.0.0.0
Oracle Audit Vault and Da...	12.2.0.0.0

- On the Confirmation dialog, click **Close**.

To monitor the undeployment operation, click **Show Status**.

To undeploy a plug-in in EM CLI, use the following command:

```
$emcli undeploy_plugin_from_server
-plugin="plug-inId"
[-sys_password="sys_password"]
[-dbUser="dbUser"]
[-dbPassword="dbPassword"]
```

For example:

```
$emcli undeploy_plugin_from_server -plugin="oracle.sysman.empa" -
sys_password="sys_password"
```

Note

- SYS is the default Management Repository admin user.

Starting with Enterprise Manager 13c Release 5 Update 15 or higher, you can undeploy plug-ins using a non-SYS user as the Management Repository admin user. In this case, you need to provide the credentials of the non-SYS admin user using the arguments: `-dbUser` and `-dbPassword`. If the `-dbPassword` argument is not provided, it will be prompted when `-dbUser` is passed.

Once a lifecycle management operation, such as patching, plug-in deployment or undeployment, is performed using a non-SYS user, you cannot use the SYS user to undeploy plug-ins anymore.

- When a metadata plug-in is undeployed/redeployed, it is recommended that you run the following command. The command should be run in each OMS environment instance.

```
$emcli metric_control -command=flush_metadata_cache
```

If you want to undeploy only the plug-ins from the OMS, and not the entire Enterprise Manager system, then use the Plug-ins page within the Enterprise Manager console. **Do NOT use runInstaller to undeploy only the plug-ins.**

Undeploying Plug-Ins from Oracle Management Agent

To undeploy plug-ins from the Management Agent, follow the steps below:

Note

- These steps are applicable for obsolete and deprecated plug-ins as well.
- Undeploying a plug-in from Management Agent removes all the targets that were monitored by the plug-in.
- Undeployment of a plug-in from the Management Agent restarts the Management Agent. The Management Agent does not monitor any target during downtime.

1. From the **Setup** menu, select **Extensibility**, then select **Plug-ins**.
2. On the Plug-ins page, select the plug-in you want to undeploy, and from the **Actions** menu, select **Undeploy From**, then select **Management Agent**.
3. In the Undeploy Plug-in From Management Agent dialog, click **Add** and add the Management Agents from which you want to undeploy the plug-in. Click **Continue**. Then click **Undeploy**.
4. On the Confirmation dialog, click **Close**.

To monitor the undeployment operation, click **Show Status**.

Note

Undeploying a plug-in from Management Agent removes all the targets that were monitored by the plug-in.

Undeployment of a plug-in from the Management Agent restarts the Management Agent. The Management Agent does not monitor any target during downtime.

To undeploy a plug-in using EM CLI, use the following command:

```
$emcli undeploy_plugin_from_agent  
-plugin="pluginId"  
{-agent_names="agent1[:agent2...]" | -all_discovery_only_agents}
```

To undeploy all versions of `oracle.sysman.db2` plug-ins from all Management Agents where only Discovery Plug-ins are deployed, use the following command:

```
$emcli undeploy_plugin_from_agent -plugin=oracle.sysman.db2 -  
all_discovery_only_agents
```

Advanced Operations with Plug-Ins

This section explains the following:

- [Re-deploying Plug-Ins on Oracle Management Agent](#)
- [Deploying Plug-In Patches While Deploying or Upgrading Management Agent \(Create Custom Plug-In Update\)](#)

Re-deploying Plug-Ins on Oracle Management Agent

Using re-deploy option, you can re-deploy plug-ins on Oracle Management Agent. The re-deploy plug-in option reconfigures the same plug-in on the Management Agent, and does not change the configuration details.

```
$emcli redeploy_plugin_on_agent  
  
{-agent_names="agent1[:agent2...]" | -group_name="group1"}  
  
-plugin="plug-in_id:version"  
  
[-redploy_noprompt]
```

Note

While using this option, note that the existing plug-in home will be overwritten, and all applied patches will be lost.

The re-deploy wizard displays the following warning message:

Re-deployment of a plug-in overwrites the existing OracleHome of a plug-in and you will lose any patch(es) that has been applied on plug-in OracleHome.

However, if you have enabled `-redploy_noprompt` option, then the warning message will not be displayed.

To continue, click **Yes**.

The redeploy command cannot be used on multiple Management Agents without having Custom Plug-in Update for a plug-in.

Note

After a metadata plug-in is redeployed, it is recommended that you run the following command.

```
$emcli metric_control -command=flush_metadata_cache
```

The command should be run on all OMS instances.

Deploying Plug-In Patches While Deploying or Upgrading Management Agent (Create Custom Plug-In Update)

When a new plug-in is released, it can be downloaded using Self-update. If there are defects with the Management Agent plug-ins, Oracle then releases O-patch style patches. While plug-ins get deployed automatically during target discovery on Management Agents, patches for the plug-ins have to be applied on each plug-in manually.

Custom plug-in update is the user copy of the plug-in, along with patches applied to it. Using the Create Custom Plug-In Update command allows you to create a custom copy of plug-in along with the patches applied in self update. Once the patches are applied, you can create a custom plug-in update of the plug-ins on that Management Agent. The custom plug-in update then becomes a gold image for that plug-in with all the patches applied on that Oracle Home, along with the base plug-in binaries.

After the Custom Plug-in Update is created, any plug-in deployment operation for the plug-in on any Management Agent, using either UI or EMCLI, the new custom copy will be deployed instead of the Oracle supplied version. In this way you don't have to reapply the plug-in patches manually on each plugin home of agent. This custom plug-in image is also used by Agent deployment to upgrade activity so that the plug-ins getting deployed on these agents are with the patch included.

There are two methods of creating Custom Plug-in Update. The following sections describe the two methods.

- [Creating Custom Plug-In Update Using EMCLI](#)(recommended)

- [Creating Custom Plug-In Update Using EDK](#)

Creating Custom Plug-In Update Using EMCLI

To create a custom plug-in update, follow these steps:

1. Select a test Management Agent which is up and running on which the preferred plug-in is already deployed. Apply any patches that you want to apply on this plug-in.
2. Perform the required testing.
3. Create a custom plug-in update using the following command:

```
$emcli create_custom_plugin_update  
-agent_name="agent_name"  
-plugin_id="plugin_id"
```

Note

To overwrite and update your current custom plug-in update that is stored in a repository, use the `overwrite` option.

```
$emcli create_custom_plugin_update  
-agent_name="agent_name"  
-plugin_id="plugin_id"  
[-overwrite]
```

This command creates and imports a custom plug-in update from an existing Management Agent where the selected plug-in is deployed. The custom plug-in update will be used for all subsequent plug-in deployments on any Management Agent, in place of Oracle supplied versions.

Custom plug-in update is created as per plug-in type. If a custom plug-in update is created, and after three days, a patch is applied, in order to include the patch, the custom plug-in update will have to be created again.

To view a list of all Custom Plug-in Updates created, run the following command.

```
$emcli list_custom_plugin_updates
```

To view a a list of patches included in a particular Custom Plug-in Update, run the following command.

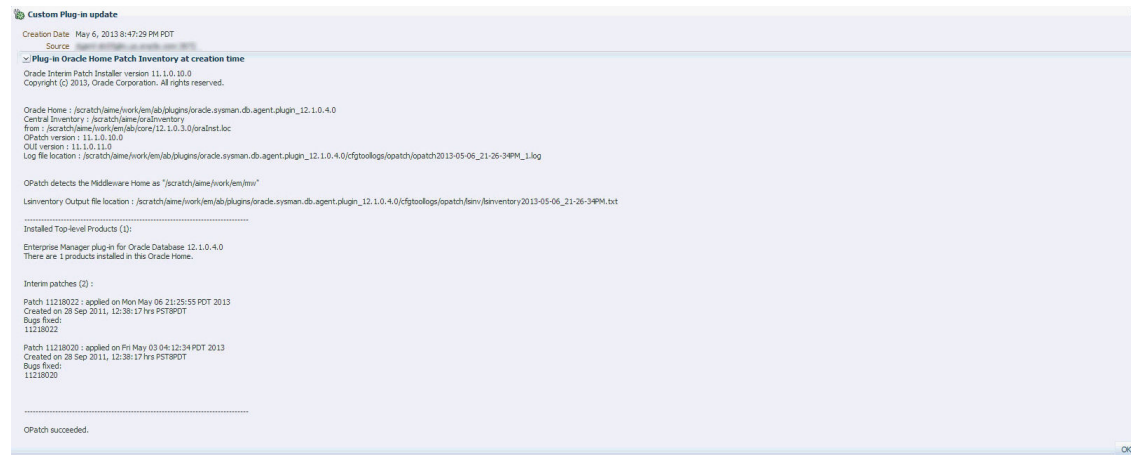
```
$emcli list_patches_in_custom_plugin_update -plugin=<plugin_id>:<version> [-  
discovery]
```

On the Plug-in Manager console, when you select a plug-in, if a Custom Plug-in Update exists, an icon is displayed beside the version identifier, indicating that that particular plug-in version is customized in the environment, with a list of patches. [Figure 4-9](#) displays the Custom Plug-in Update icon. Once the custom plug-in update exists, it will be used by the Management Agent for deployment and upgrade automatically.

Figure 4-9 Custom Plug-in Update Icon

Plug-in ID	oracle.sysman.db	Versions Downloaded	12.1.0.5.0 , 12.1.0.4.0 , 12.1.0.3.0 , 12.1.0.2.0 [u120704], 12.1.0.1.0 [u111221]
Vendor	oracle	Supported versions on Management Agent	12.1.0.4.0 , 12.1.0.3.0 , 12.1.0.2.0 [u120704]
Version on Management Server	12.1.0.4.0	Description	Enterprise Manager for Oracle Database provides comprehensive management for Oracle Database and related targets s
Latest Available Version	12.1.0.5.0		
Versions Deployed On Management Agents			Custom plug-in update exists. Click to view details.

When you click the Custom Plug-in Update icon, the page that displays the information on Custom Plug-in Update is displayed. [Figure 4-10](#) displays the Custom Plug-in Update information page.

Figure 4-10 Custom Plug-in Update Information Page

Creating Custom Plug-In Update Using EDK

To create custom plug-in update using EDK, follow these steps.

1. Download EDK, using the UI or EMCLI, on the Management Agent Host.

To download EDK using UI, from the **Setup** menu, select **Extensibility**, and then select **Development Kit**.

To download EDK using EMCLI, run the following command.

```
$emcli get_ext_dev_kit
```

2. Run the following command.

```
$empdk create_custom_plugin_update -out_dir <output_dir>
-agent_state_dir <agent_state_dir>
-agent_oracle_home <agent_oracle_home>
-plugin_id <plugin_id>
```

For help with empdk commands, run the following command.

```
$/empdk -help
```

The plug-in update is saved to on a local directory as a .zip file. The .zip file has to be copied to an OMS instance. Once the .zip file is created, from the OMS Home, run the following command to import the custom plug-in update.

```
$emcli import_plugin_update -archive=<archive path>
```

On the Plug-in Manager console, when you select a plug-in, if a Custom Plug-in Update exists, an icon is displayed beside the version identifier, indicating that particular plug-in version is customized in the environment, with a list of patches.

Troubleshooting

This section contains information on troubleshooting plug-in related issues. The following sections are covered in this section:

- [Understanding Plug-In Homes](#)
- [Troubleshooting OMS Plug-In Deployment and Upgrade Issues](#)
 - [Troubleshooting OMS Plug-In Deployment Issues](#)
 - [Rollback and Resume OMS Plug-In Upgrade](#)
- [Troubleshooting Management Agent Plug-In Deployment, Upgrade, and Blocked Issues](#)
 - [Troubleshooting Management Agent Plug-In Deployment Issues](#)
 - [Troubleshooting Management Agent Plug-In Upgrade Issues](#)
 - [Resolving a Plug-in Mismatch on a Management Agent](#)
 - [Running a Plug-in Mismatch Job to Resolve All Plug-in Mismatches](#)

Understanding Plug-In Homes

Plug-in homes are essentially directories under Oracle homes that are dedicated for plug-ins. The plug-in home for plug-ins deployed to the OMS is different from the plug-in home for plug-ins deployed to the Management Agent. Since plug-in homes are registered in the oraInventory, they should not be manually deleted or manipulated.

[Figure 4-11](#) shows the plug-in home directory for plug-ins deployed to Enterprise Manager 24ai (for OMS).

Figure 4-11 Plug-In Home for Enterprise Manager 24ai (for OMS)

```
<OMS home>
|_____bin
|_____coherence
|_____plugins
|_____plugging_common
```

[Figure 4-12](#) indicates the plug-in home directory for plug-ins deployed to Management Agents of 24ai.

Figure 4-12 Plug-In Home for Oracle Management Agents 24ai

```
<Agent Oracle home>
|_____bin
|_____jdk
|_____plugins
```

Troubleshooting OMS Plug-In Deployment and Upgrade Issues

If the deployment of a new plug-in fails, the system automatically recovers. When the automatic recovery is complete, all OMS instances are started. If the upgrade of an existing plug-in fails, manual system recovery is required.

This section provides troubleshooting tips related to the following topics:

- [Troubleshooting OMS Plug-In Deployment Issues](#)
- [Rollback and Resume OMS Plug-In Upgrade](#)

Troubleshooting OMS Plug-In Deployment Issues

If plug-in deployment to the OMS fails, first check the details of the deployment, using the following commands.

- If the OMS is down, use the following command.

```
$emctl status oms -details
```
- If the OMS is running, use the following command.

```
$emcli get_plugin_deployment_status
```

Note

When the status of the OMS is displayed, review the log files that are displayed in the output.

It is recommended that you take a backup of the Repository in case of a failure in the Recovery.

Review the `pluginca` log file available in the following location. Use them to debug the issue, and if you raise a service request to Oracle Support, then make sure you append these to the service request.

```
$<OMS_HOME>/cfgtoollogs/pluginca/*
```

Note

When you install an additional OMS by cloning an existing, running OMS instance, the plug-in deployed to the source OMS are automatically carried over to the cloned OMS as well. Therefore, you do not have to redeploy the plug-ins on the cloned OMS.

In case of multi OMS environment, the `OMS_HOME` in the log file path indicates the root folder of the OMS where the failure occurs.

For information about installing an additional OMS, refer to the *Oracle Enterprise Manager Basic Installation Guide*.

Rollback and Resume OMS Plug-In Upgrade

If plug-in upgrade fails, then do one of the following:

- Raise a Service Request to find out if there is a possibility of recovering from the current Management Repository.
- Rollback to the latest backup of the Management Repository.
- If you have not taken a backup of the Management Repository, diagnose and resolve the issue that is causing the plug-in upgrade to fail.

Then, run the following command to resume the plug-in upgrade:

```
$<OMS_HOME>/bin/emctl resume_plugin_upgrade
```

This command automatically detects and resumes the last failed upgrade session. Once the plug-in upgrade succeeds, the OMS restarts automatically. The same deployment ID is updated with the current status of the operation. In case of a multi-OMS environment, the plug-in upgrade happens on the first OMS, and then on all other additional OMS instances.

- If flashback is enabled, the section number will be printed.

Troubleshooting Management Agent Plug-In Deployment, Upgrade, and Blocked Issues

This section provides troubleshooting tips related to the following topics:

- [Troubleshooting Management Agent Plug-In Deployment Issues](#)
- [Troubleshooting Management Agent Plug-In Upgrade Issues](#)
- [Resolving a Plug-in Mismatch on a Management Agent](#)
- [Running a Plug-in Mismatch Job to Resolve All Plug-in Mismatches](#)

Troubleshooting Management Agent Plug-In Deployment Issues

If plug-in deployment to the Management Agent fails, then review the log file available in the following locations.

```
agent_inst/sysman/log/*
```

```
agent_inst/sysman/registry.xml
```

```
agent_inst/install/logs/*
```

Troubleshooting Management Agent Plug-In Upgrade Issues

If plug-in upgrade fails, then review the log file available in the following locations.

- To review the log files using the UI, follow these steps.
 1. From the **Setup** menu, select **Extensibility**, and then select **Plug-ins**.
 2. Select the preferred plug-in, and review the information displayed in the **Recent Deployment Activities** tab.
 3. Click the link in the **Action** column for the preferred Management Agent. From the **Deployment Steps** tab, select the job name. Selecting the job name opens the job details wizard.
- The detailed logs for Management Agent upgrade and deployment are available at the following location.

```
agent_inst/install/logs/agentplugindeploy_N.log
```

In the aforementioned location, N refers to the internal ID. Check the latest log files in the location.

- While filing an SR, upload the following log files.

agent_inst/install/logs/*

agent_inst/sysman/log/*

agent_inst/sysman/registry.xml

Resolving a Plug-in Mismatch on a Management Agent

When there is a plug-in version mismatch on the Management Agent and OMS, and in this situation the Management Agent is restarted (bounced), the Management Agent is moved to the "Blocked" state.

If a Management Agent is in the Blocked state due to a plug-in mismatch, follow the steps below to resolve the mismatch error:

1. From the Setup menu, select **Manage Enterprise Manager** and then click **Agents**.
2. In the Status column look for the Management Agents which are in the **Blocked** state.
3. Click on the Management Agent name link to open the agent home page.
4. In the Summary pane look for the Status row and click the **Resolve Mismatches** icon next to "Blocked."
5. In the Plug-in Mismatch page review all the plug-in mismatches discovered on the agent and click **Resolve Mismatches**.
6. Click **OK** in the Confirmation pop-up window.

A confirmation message with the status is displayed.

Running a Plug-in Mismatch Job to Resolve All Plug-in Mismatches

When there is a plug-in version mismatch on the Management Agent and OMS, and in this situation the Management Agent is restarted (bounced), the Management Agent is moved to the "Blocked" state.

Follow the steps below to run a job to find any plug-in mismatches in Management Agents and to resolve the issue/s if there are any mismatches:

1. From the **Enterprise** menu, select **Job**, and then click **Activity**.
2. Click **Create Job**.
3. Select **Plug-in Mismatch Check** from the Job Type column and click **Select**.
4. Enter a name for the job in the **Name** field.
5. From the Target section click **Add**.
6. Select the Management Agents on which you want to run the job and click **Select**.
7. Click **Parameters** tab.
8. From the **Fix Mismatch** drop-down list select **True**.

Note

When the **Fix Mismatch** field is set to **True**, the job may shut down the selected Management Agents if the plug-in mismatch is found. Exercise caution when setting this option.

9. Click **Submit** to run the job.
10. After the job has completed click on the job name link to open the Job page.

The Output Log provides the details of the job run and the action taken to resolve the plug-in mismatches (if any).

5

Patching and Updating Enterprise Manager

Patching and updating Enterprise Manager allows you to expand its capabilities when new features become available and improve the performance and security of your Enterprise Manager deployment.

The following topics are covered:

- [Updating Enterprise Manager](#)
- [Patching Oracle Management Service and the Repository](#)
- [Patching Oracle Management Agents](#)

Updating Enterprise Manager

The Self Update feature allows you to expand Enterprise Manager's capabilities by updating Enterprise Manager components whenever new or updated features become available. Updated plug-ins are made available via the Enterprise Manager Store, an external site that is periodically checked by Enterprise Manager to obtain information about updates ready for download.

This chapter contains the following sections:

- [Using Self Update](#)
- [Setting Up Self Update](#)
- [Applying an Update](#)
- [Accessing Informational Updates](#)
- [Acquiring or Updating Management Agent Software](#)

Using Self Update

The Self Update feature is accessed via the Self Update home page, a common dashboard used to obtain information about new updates and a common workflow to review, download and apply the updates. The Self Update console frees you from having to monitor multiple channels to get informed about new updates that are available from Oracle. The Self Update console automatically informs you whenever new updates are made available by Oracle. Only those updates that are applicable to your site are shown, eliminating the need to wade through unrelated updates.

What Can Be Updated?

Specific updates authored by Oracle that are usually bundled with specific Enterprise Manager releases can be updated via Self Update. Some examples are Oracle authored Management Plug-ins or Deployment Procedures. In general, Oracle-supplied entities are read-only. You can create a copy and customize the copy as per your needs but you cannot modify the original Oracle-supplied entity.

These entities can also be published on Oracle Web sites such as My Oracle Support (MOS). You can download and import the entity archive into their Enterprise Manager deployment using specific import features provided by the updatable entity.

Entity Types That Can Be Updated

Examples of updatable entity types are:

- Management Agents
- Management Plug-ins
- Management Connectors
- Database Profiles and Gold Images
- Application Server Profiles and Gold Images
- Provisioning Bundles
- Enterprise Manager Deployment Prerequisite Checks
- Compliance Content
- Diagnostic Checks

Setting Up Self Update

Before you can use the Self Update feature, you must satisfy these prerequisites:

- My Oracle Support credentials have been set up using the SYSMAN user. This is required to enable entities to be downloaded from the My Oracle Support site.
- The Software Library (also known as the local store) has been configured. Updates are downloaded to this local store before being deployed into Enterprise Manager.

Review the following sections for instructions on setting up Self Update:

- [Setting Up Enterprise Manager Self Update Mode](#)
- [Assigning Self Update Privileges to Users](#)
- [Setting Up the Software Library](#)
- [Setting My Oracle Support Preferred Credentials](#)
- [Registering the Proxy Details for My Oracle Support](#)
- [Setting Up the EM CLI Utility \(Optional\)](#)

Setting Up Enterprise Manager Self Update Mode

In order to set up or modify the Enterprise Manager Self Update feature, you must have Enterprise Manager Super Administrator privileges.

1. Log in to Enterprise Manager as an administrator with Super Administrator privileges.
2. From the **Setup** menu, select **Extensibility**, then select **Self Update**. The Self Update console appears with the default setup displayed.
3. From the **General** status area, click the **Connection Mode** status to set either offline or online mode. Enterprise Manager takes you to the Patching Setup page to specify online and offline settings.

Note

When Enterprise Manager runs in Online mode, it does not upload any data to MOS. It only uses MOS to download the latest updates.

4. Once the desired connection mode has been selected, return to the Self Update console. From here you can select entity types and schedule updates from the Enterprise Manager Update Store.

Assigning Self Update Privileges to Users

Enterprise Manager administrators must have the requisite privileges to use the Self Update feature. The Enterprise Manager Super Administrator must assign the following Self Update roles/privileges to these administrators:

- *View any Enterprise Manager Update*—User can view the Self Update console and can monitor the status of download and apply jobs.
- *Self Update Administrator*—User can schedule download and apply jobs. User can also suppress/unsuppress updates. This privilege implicitly contains the View any Enterprise Manager Update privilege.
- *EM_INFRASTRUCTURE_ADMIN*—User can perform all self update operations. This role implicitly contains the *Self Update Administrator* privilege.

By default, the Super Administrator will be granted EM_INFRASTRUCTURE_ADMIN privilege.

To assign Self Update privileges to regular Enterprise Manager administrators:

1. From the **Setup** menu, select **Security**, then select **Administrators**.
2. Select an administrator and click **Edit**.
3. From the Roles page, assign the appropriate Self Update roles.

Setting Up the Software Library

The Software Library is a repository that stores 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. In the context of applying updates, it is the "local store" that entities are downloaded to before deployment.

If the Software Library is not already set up in your environment, see Chapter 8, "Configuring Software Library," for instructions on the various ways you can configure the Software Library.

Setting My Oracle Support Preferred Credentials

To set the preferred credentials that must be used by the OMS to connect to My Oracle Support (MOS), follow these steps:

1. From the **Setup** menu, select **My Oracle Support**, then select **Set Credentials**.
2. Specify the user name and the password.
3. Click **Apply**.

Registering the Proxy Details for My Oracle Support

Enterprise Manager 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. You can register the proxy details for My Oracle Support using the My Oracle Support Proxy Settings page.

To register the proxy details for My Oracle Support (MOS), follow these steps:

1. From the **Setup** menu, select **Proxy Settings**, then select **My Oracle Support**.
2. If you want the OMS to connect to MOS directly, without using a proxy server, follow these steps:
 - a. Select **No Proxy**.
 - b. Click **Test** to test if the OMS can connect to MOS directly.
 - c. If the connection is successful, click **Apply** to save the proxy settings to the repository.
3. If you want the OMS to connect to MOS using a proxy server, follow these steps:
 - a. Select **Manual proxy configuration**.
 - b. Specify the proxy server host name for **HTTPS** and an appropriate port value for **Port**.
 - c. If the specified proxy server has been configured using a security realm, login credentials, or both, select **Password/Advanced Setup**, then provide values for **Realm**, **User Name**, and **Password**.
 - d. Click **Test** to test if the OMS can connect to MOS using the specified proxy server.
 - e. If the connection is successful, click **Apply** to save the proxy settings to the repository.

Note

- If you are using a proxy server in your setup, ensure that it 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 servers are not supported. If you are using an NTLM based Microsoft proxy server, to enable access to the above sites, add the above URLs to the Unauthenticated Sites Properties of the proxy server.
- The MOS proxy server details specified on the MOS Proxy Settings page apply to all the OMS in a multi-OMS environment.

Setting Up the EM CLI Utility (Optional)

If you plan to apply software updates in offline mode, you will need to use the Enterprise Manager Command Line Utility, or EM CLI, to import entity archives for deployment to Enterprise Manager.

EM CLI is set up on OMS out-of-box. If you need to set up EM CLI on another machine managed by Enterprise Manager, a page is provided in the Enterprise Manager console with instructions on setting up EM CLI. Access the page by appending `/console/emcli/download` to the URL used to access the Enterprise Manager console:

`https://em_host:em_port/em`

For example:

`https://em_host:em_port/em/console/emcli/download`

Applying an Update

The process for applying updates is essentially as follows:

- Check for the latest updates available from Oracle.
- Download the updates you want to apply to the Software Library.
- Apply the update.

Review the following sections to learn how to apply an update:

- [Applying an Update in Online Mode](#)
- [Applying an Update in Offline Mode](#)

Applying an Update in Online Mode

Updates must be downloaded to the Software Library (the local store) before they can be applied. You can review the latest available updates from the Self Update console.

Note that Enterprise Manager must have access to the Enterprise Manager Store via the Internet to download available updates. If this access is not possible, you can download entities in offline mode. See [Applying an Update in Offline Mode](#) for details.

1. From the **Setup** menu, select **Extensibility**, then select **Self Update**.
2. Click **Check Updates** to submit a job to check for new updates from Oracle. Click **OK** to close the confirmation message.
3. When the job completes, select the desired entity type, then select **Open** from the **Actions** menu. The entity type page appears.
4. Select an update from the list of available updates.
5. Click **Download**. The Schedule Download dialog appears.
6. Select when to download the update. Note that multiple downloads can be scheduled simultaneously.

The following options are available:

- Immediately
 - Later (specified time)
 - Whether or not to send a notification when the download is complete
7. Click **Select**. An Enterprise Manager job is created to download the update to the Software Library.

Enterprise Manager starts downloading the archive from the Oracle Enterprise Manager store. Wait for the download to complete. (When in offline mode the system starts reading from the specified location.)

When the download is complete, Enterprise Manager displays the Confirmation page.

Note

The page is not refreshed automatically. Click the refresh icon to view the updated download status.

8. Once an entity has been downloaded to the Software Library, it is ready to be applied to your installation. Select an update from the list whose status is **Downloaded**, then click **Apply**.

Note that the application process varies according to the entity type:

- For connectors, diagnostic checks, and compliance content, clicking **Apply** will install the update to Enterprise Manager. No further action is required.
- For plug-ins, you will be redirected to the plug-in deployment page.
- For provisioning bundles, you will need to exit the Enterprise Manager console, run Opatch and other commands via a terminal, and then restart the OMS.

Applying an Update in Offline Mode

Under certain circumstances, such as in high security environments, an active Internet connection between Enterprise Manager and the Enterprise Manager Update Store may not be available. In such situations, the Self Update feature can be used in offline mode.

The update process still requires that a computer exist at your site that has Internet access, as a connection to the Enterprise Manager Update Store is still required to obtain the updates. Update files from this computer can then be transferred to a computer behind your firewall.

The generic offline mode update procedure is as follows:

1. Ensure that Enterprise Manager is set to offline mode. From the **Setup** menu, select **Provisioning and Patching**, then select Offline Patching.
2. Change the setting for Connection to **Offline**.
3. Click **Check Updates** on the Self Update home page. A message is displayed that contains the URL to be accessed to download a catalog of all updates.
4. From an Internet-enabled computer, download the catalog file using the aforementioned URL.
5. Copy the downloaded file to the Oracle Management Service host or the Management Agent host you will deploy the update to.
6. Run the `emcli import_update_catalog` command to import the file into the Oracle Management Service instance or the Management Agent you want to update.
7. Review the update from Self Update Home and click **Download** in the **Actions** menu. A message displays with a URL and instructions.
8. Click **Apply** in the **Actions** menu to apply the update.

Accessing Informational Updates

The Self Update feature also serves as a news feed, providing new product announcements, news stories, industry updates, and any number of other items of interest to the Oracle community. These informational updates occur on an ad hoc basis and typically include useful links where you can obtain additional information and download items.

1. From the **Setup** menu, select **Extensibility**, then select **Self Update**.

2. On the Self Update page, click the **Informational Updates** link at the top-right corner. The link includes the number of new updates. A number appears only if there are new (unread) updates.
3. Select an update notification in the table and click **Details**.
A popup appears describing the new product and listing applicable links.
4. Click **OK** to close the details display and return to the table of announcements.
By default, the table displays only unread announcements. You can choose to display all or only read announcements. You can also toggle selected items between read and unread states. Note that if you mark an item as read, you are doing so for all users. A warning to this effect appears.

Acquiring or Updating Management Agent Software

Management Agent software for the various platforms (operating systems) supported by Enterprise Manager can be downloaded to the Software Library using the Self Update console. Once a Management Agent is persisted to the Software Library, it can be installed on host machines that you want to bring under management using the Add Host Targets wizard.

For instructions on obtaining Management Agent software in both online and offline modes, see the section "*Meeting Management Agent Software Prerequisites*" in the *Oracle Enterprise Manager Basic Installation Guide*.

Patching Oracle Management Service and the Repository

OMSPatcher automates the patching process by generating custom patching instructions based your particular environment and then automatically applies the patch. To increase patching flexibility and minimize downtime, OMSPatcher provides a zero downtime patching option in addition to traditional patching.

This chapter covers the following topics:

Traditional Patching (Normal downtime patching)

- [OMSPatcher Automation](#)
- [Required OMSPatcher Parameters](#)
- [Prerequisites for Running OMSPatcher](#)
- [Using OMSPatcher](#)
- [Patching with Non-SYS User \(Admin User\)](#)
- [OMSPatcher Command Syntax](#)

Zero Downtime Patching (Online patching)

- [Zero Downtime Patching](#)
 - [Prerequisites](#)
 - [Limitations](#)
 - [EM Monitoring When Performing Zero Downtime Patching](#)
- [OMSPatcher Command Updates](#)
- [Zero Downtime Patching Workflow](#)
- [Patching Use Cases](#)

- [Applying MRS Artifacts](#)
- [Post-Patching Verification](#)

Other Patching Method

- [Holistic Patching](#)

Troubleshooting OMS Patching

- [Troubleshooting](#)
- [OMSPatcher Session Resume](#)

OMSPatcher Automation

With OMSPatcher, you can automatically patch a typical OMS configuration (core, plug-in homes) with minimal intervention.

OMSPatcher performs many of the pre-patch checks such as:

- Configuration-based prerequisite checks
- Patch-based binary prerequisite checks

OMSPatcher performs end-to-end configuration patching. Configuration patching is the process of patching a target based on its configuration. By incorporating the configuration information into the patch process, OMSPatcher is able to simplify patching tasks by automating most of the steps.

Supported OMS Configurations and OMSPatcher Patchability

- Single OMS – OMS application that runs from a single OMS instance of the system. OMSPatcher performs patching and deployment operations
- Multiple OMS – OMS applications that run on two or more hosts. The OMSes are connected by the Oracle WebLogic domain and separate managed servers. There is a one-to-one mapping between the managed servers and the separate OMS bits residing on a particular machine. There are two ways in which patches are applied on a multiple OMS setup.
 - Automated: A job is submitted to patch the add OMSes after the primary/first OMS patching is completed.
 - Manual: OMSPatcher provides auto-generated bash scripts (one per OMS instance) for UNIX based systems. OMSPatcher on Linux skips automatic patching on add OMSes if the `-skipautopatch_addoms` parameter is passed (one per OMS instance expect primary OMS).

Note

The `-skipautopatch_addoms` parameter is allowed only for traditional patching (non-ZDT patching). The script is created to patch the add OMSes after the primary/first oms is patched.

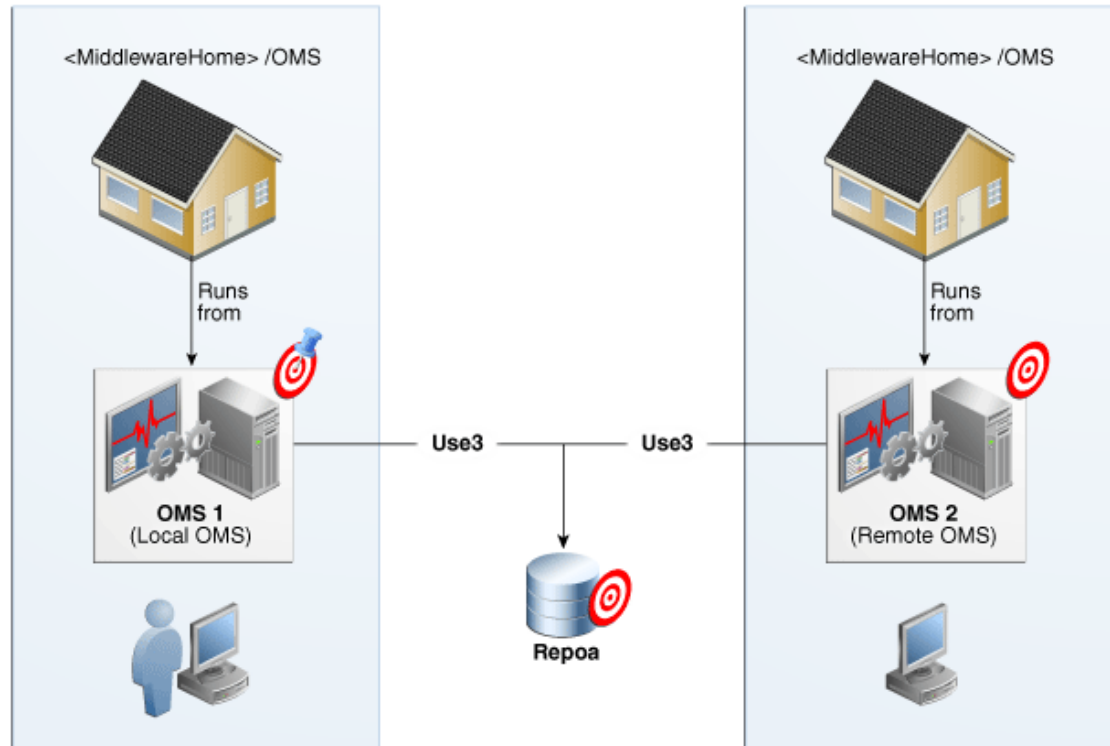
The administrator needs to follow the steps given by OMSPatcher.

- Single Instance Database or Real Application Cluster - shared or Real Application Cluster (RAC)

Example: Multi-OMS System

The following figure illustrates a multi-OMS deployment. The following terms are used:

- *Administrator*: Person installing patches to the OMS core and plug-in homes.
- *Local OMS*: OMS instance on which the administrator runs OMSPatcher.
- *Add OMS*: OMS instances on other machines (within the same OMS domain as the local OMS) where the administrator has not started any patching operations.

Figure 5-1 Simple Multi-OMS System

For a single OMS system (primary), OMSPatcher will execute the patching steps. For a multi-OMS UNIX system, a job is automatically submitted to deploy the patches. If you need to deploy the patches manually, OMSPatcher generates bash scripts for execution, one per OMS instance for all OMSes (**except the primary OMS**); follow the instructions given by OMSPatcher to find those scripts.

Oracle Universal Installer Inventory Configurations (OUI)

Apart from the target or instance-based configuration, OMSPatcher utilizes installation configuration relationships established in the OUI inventory as core and plug-in feature-sets. A typical OMS home is organized as follows:

```
<Middleware Home>
|
|--- <CORE_BITS>
|
|...
|--- OMSPatcher
|       |
|       |--- jlib
|       |--- oms
```

```

|
|— omspatcher
|— omspatcher.bat
|— restoring_env.txt
|— scripts
|— version.txt
|— wlskeys
|
|— OPatch
|
|— auto
|— bin
|— docs
|— emdpatch.pl
|— jlib
|— ...
...
|
|— plugins
|
|— backup
|— oracle.em.savf.oms.plugin_13.5.1.0.0
|— oracle.em.smis.oms.plugin_13.1.1.0.0
|— tmp
...

```

Supported Patch Format

Enterprise Manager patches have been converted to a *System patch* format in order to support patch automation.

What is a System Patch?

A System patch contains several sub-patches whose locations are determined by a file called *bundle.xml* in the top level directory of the patch. The sub-patches are intended for different sub-systems of a system that correspond with the OMS core and plug-in home organization.

A typical System patch format is organized as follows:

```
<System patch location - directory>
|_____ Readme.txt (or) Readme.html
        bundle.xml
        automation
            |_____ apply_automation.xml
            |_____ rollback_automation.xml
Sub-patch1
    |_____ etc
        |_____ config
            |_____ inventory.xml
            |_____ actions.xml
            |_____ artifact_apply.xml
            |_____ artifact_rollback.xml
    |_____ files/Subpatch1 'payload'
Sub-patch2
    |_____ etc
        |_____ config
            |_____ inventory.xml
            |_____ actions.xml
            |_____ artifact_apply.xml
            |_____ artifact_rollback.xml
```

```
|_____ files/Subpatch1 'payload'
```

Supported Patching Methodologies

OMSPatcher supports rolling mode only for System patches without any automation (binary-only patching through OMSPatcher). For all other artifacts, such as Metadata Registration Service (MRS) or SQL, OMSPatcher only supports complete system downtime patching operations, refer as **Traditional Patching**.

Other patching methodologies:

- **Zero Downtime Patching**
OMSPatcher also supports Zero Downtime patching which allows the patching process to take place while the OMS is up and running reducing the system downtime. For more information, see [Zero Downtime Patching](#).
- **Holistic Patching**
This methodology is used for applying the Enterprise Manager quarterly Critical Patch Update (CPU patches). For information, see [Holistic Patching](#).

Refer to the patch README for the explicit information on supported patching methodologies.

Required OMSPatcher Parameters

OMSPatcher for the Enterprise Manager OMS will prompt for the following input parameters when performing patching operations. These parameters were determined at the time of Enterprise Manager installation.

- Oracle WebLogic Admin Sever URL & port number
- Oracle WebLogic Administration Server username
- Oracle WebLogic Administration Server password
- Oracle Database username
- Oracle Database user password
- SYSMAN user password

Because OMSPatcher requires this input for each patching operation, OMSPatcher provides the ability to encrypt the username and password via WebLogic encryption APIs and pass this information using a property file when running all OMSPatcher operations. The next section discusses how to create a property file.

Creating a Property File

The automated patching functionality achieved using OMSPatcher expects WebLogic Administration Server URL and credentials as an input for patching and configuration detection operations. Primarily, the WebLogic Administration server is the host that manages the Managed Server where the OMS instance is deployed. If you do not want to set the credentials every time you are prompted while patching the OMS, you can update the property file. OMSPatcher allows you to repeatedly provide the inputs using property file option.

Note

If the OMSes are configured with virtual hostnames, you first need to set the following environment variable before executing the `createkeys.sh` command (Step 1).

```
export WLST_PROPERTIES="-  
Dweblogic.security.SSL.ignoreHostnameVerification=true"
```

1. Navigate to the Oracle home and run the following script to create the WebLogic encrypted configuration and key files.

On UNIX:

```
$ OMSPatcher/wlskeys/createkeys.sh -oh <ORACLE_HOME> -location <location to  
put the encrypted files>
```

On Windows:

```
$ OMSPatcher\wlskeys\createkeys.cmd -oh <ORACLE_HOME> -location <location to  
put the encrypted files>
```

When prompted, enter the credentials of the Oracle WebLogic Administration Server that manages the Managed Server on which OMS instance is deployed. Two files are generated with the file names: `config` and `key`.

2. Create the property file with the following entries:

```
AdminServerURL=t3s://<host address from where admin server is running>:<port of the  
admin server>  
AdminConfigFile=<'config' file location>  
AdminKeyFile=<'key' file location>  
dbUser=<db user>  
dbPassword=<db password>
```

The values for host address and port of admin server can be located by running `emctl status oms -details` on an Oracle Home.

Example

```
./emctl status oms -details  
Oracle Enterprise Manager 24ai Release 1  
Copyright (c) 1996, 2024 Oracle Corporation. All rights reserved.  
Console Server Host : host01.example.com  
HTTP Console Port : 7790  
HTTPS Console Port : 7804  
HTTP Upload Port : 4890  
HTTPS Upload Port : 4904  
EM Instance Home : /u01/em/mw/gc_inst/em/EMGC_OMS1  
OMS Log Directory Location : /u01/em/mw/upvtxml/mw/gc_inst/em/EMGC_OMS1/  
sysman/log  
OMS is not configured with SLB or virtual hostname  
Agent Upload is locked.  
OMS Console is locked.  
Active CA ID: 1  
Console URL: https://host01.example.com:7804/em  
Upload URL: https://host01.example.com:4904/empbs/upload
```

```
WLS Domain Information
Domain Name : GCDomain
Admin Server Host : host01.example.com
Admin Server HTTPS Port: 7103
Admin Server is RUNNING

Extended Domain Name : EMExtDomain1
Extended Admin Server Host : host01.example.com
Extended Admin Server HTTPS Port: 7016
Extended Admin Server is RUNNING

Oracle Management Server Information
Managed Server Instance Name: EMGC_OMS1
Oracle Management Server Instance Host: host01.example.com
WebTier is Up
Oracle Management Server is Up
JVMD Engine is Up
```

Following is the example of how a property file (constructed by the above mentioned guidelines) should appear:

```
AdminServerURL=t3s://my_admin_server.mycompany.com:7101
AdminConfigFile=/scratch/patch/oms_install_dir/middleware/oms/config/config
AdminKeyFile=/scratch/patch/oms_install_dir/middleware/oms/config/key
dbUser=db_user
dbPassword=db_password
```

Note

To retrieve the WebLogic Administration Server URL details, run the following commands on the OMS home that you are patching:

On Unix:

```
$ORACLE_HOME/bin/emctl status oms -details
```

On Windows:

```
%ORACLE_HOME%\bin\emctl.bat status oms -details
```

The command output contains the WebLogic Administration Server details. Here is an example on how to construct the URL with these output details.

Example:

```
WLS Domain Information

Domain Name : GCDomain
Admin Server Host : my_wls.mycompany.com
Admin Server HTTPS Port: 7103
```

To construct the Administrator Server URL, use the following syntax:

```
t3s://<admin server host>:<port>
```

In this example, the URL translates as follows:

```
t3s://my_wls.mycompany.com:7103
```

Prerequisites for Running OMSPatcher

Before running an OMSPatcher patching session, you must ensure the following configuration and inventory-based prerequisites are satisfied: Configuration-based conditions that have to be honored for OMS automation is given below.

- The Enterprise Manager Software library must be configured.
- The Oracle WebLogic Administration Server that controls the OMS instance (currently to be patched) through a managed server must be up and running.
- Ensure that the Oracle Database, which houses the OMS Management Repository, and its listener are up and running.
- Ensure that you have the latest version of the OMSPatcher in the OMS platform home of each host.

If you do not have the latest OMSPatcher version, follow the instructions outlined in the My Oracle Support note [How To Upgrade Enterprise Manager OMSPatcher Utility \(Doc ID 2809842.1\)](#).

- Check your patch README to determine whether there are any specific prerequisites to be executed based on patch and patching methodologies.

Using OMSPatcher

OMSPatcher must be run from the platform home of the OMS being patched. To run OMSPatcher commands from any directory include `<ORACLE_HOME_PATH>/OMSPatcher` in the PATH environment variable. The `ORACLE_HOME` environment variable must be set as the platform home. For example:

```
omspatcher apply <patch>
```

Minimum Required OMSPatcher Version: Refer to the patch README for the required version.

Ensuring You Have the Latest Version of OMSPatcher

OMSPatcher is the patching utility that executes end to end patching procedure for OMS Patches. Ensure that the latest version of OMSPatcher is available on all instances of OMS platform homes.

To check the version of OMSPatcher residing on the system, run the following command:

```
omspatcher version
```

To get the latest OMSPatcher version, see [Doc ID 2135028.1](#) from [My Oracle Support](#).

Ensuring You Have the Latest Version of OPatch

OMSPatcher uses the OPatch utility to apply the patch. For this reason, you must ensure that you have the latest version of OPatch on all instance of OMS platform homes. To check the version of OPatch residing on the system, run the following command. Ensure to execute the command after including `ORACLE_HOME/OPatch` in the PATH environment variable.

```
opatch version
```

To download the latest version of OPatch, see [Doc ID 2728285.1](#) from [My Oracle Support](#).

Minimum Required OPatch Version: Refer to the patch README for the required version.

Patching Quickstart

Using OMSPatcher typically involves the following phases:

1. Determining Whether Your System Meets OMSPatcher System Requirements

Run `omspatcher apply -analyze`

The `apply -analyze` command simulates an OMSPatcher apply session by running all prerequisite checks, when possible, without making changes to the system (either bits or configurations). This command does not apply the patch.

See "[Prerequisites for Running OMSPatcher](#)" for additional information.

2. Determining What System Patches Currently Exist on Your System

Run `omspatcher lspatches`

See "[lspatches](#)" for more information.

3. Obtaining Patches from My Oracle Support (MOS)

OMSPatcher requires that the required platform or plug-in System patches be obtained from My Oracle Support and downloaded to the OMS instance on which OMSPatcher is to be run.

See "[My Oracle Support: Searching for Patches](#)" for more information.

4. Applying a Patch

Run `omspatcher apply <patch>`

The `apply` command applies all patches within a specified System patch to the platform home from which `omspatcher` command is run.

See "[Running omspatcher apply](#)" for more information.

5. Rollback of the System Patch

Run `omspatcher rollback -systemid <system patchid>`

If, after applying the patch, the system is not stable, the most likely cause is the patch itself. Contact Oracle Support. They will recommend that you remove the patch using the `omspatcher rollback` command.

See "[Running omspatcher rollback](#)" for more information.

My Oracle Support: Searching for Patches

The first step in the patching process is to determine what patches you need from My Oracle Support (MOS). MOS is the single source of truth for patching. You can access MOS at the following location:

<https://support.oracle.com>

Once you have logged in, you have access to interactive support tools and information that simplify searching for and obtaining the requisite patches for your Oracle environment.

My Oracle Support contains many features and capabilities that are grouped under tabs across the top of the application. Of primary interest is the *Patches and Updates* tab. From this tab you can search for the patches based on the OMS patch area (core, plug-in, or combination).

Checking System Prerequisites

Note

To run OMSPatcher commands, ensure that <ORACLE_HOME>/OMSPatcher is included in the PATH environment variable.

To make sure all prerequisite checks pass and no errors occur during the OMSPatcher patching session, Oracle recommends running the following commands on each OMS instance (in your OMS system).

```
omspatcher apply <PATCH_LOC> -analyze
```

Must be run from the System patch location (for *apply* operations)

Note

OMS systems need not be shut down when running `apply -analyze`.

Note

Check the Patch README and the instructions given for chosen patching methodologies.

OR

```
omspatcher rollback -systemid <system patchid> -analyze
```

Example 5-1 OMSPatcher rollback -analyze output

```
$omspatcher rollback -systemid 1111112 -analyze
```

```
OMSPatcher Automation Tool
```

```
Copyright (c) 2024, Oracle Corporation. All rights reserved.
```

```
OMSPatcher version : 13.9.24.1.0
```

```
OUI version : 13.9.4.0.0
```

```
Running from : $ORACLE_HOME
```

```
Log file location : $ORACLE_HOME/cfgtoollogs/omspatcher/  
opatch2024-12-02_12-30-09PM_1.log
```

```
OMSPatcher log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/  
SystemPatch/omspatcher_2024-12-02_12-30-09PM_analyze.log
```

```
Deobfuscating the related patch content in /u01/yourinst/ap_omshome.....
```

```
Deobfuscating the related patch content in /u01/yourinst/
```

```
ap_extomshome.....
```

```
Please enter OMS weblogic admin server URL(t3s://
```

```
shortterm.sub.emdev.example.com:7102):>
```

```

Please enter OMS weblogic admin server username(weblogic):>
Please enter OMS weblogic admin server password:>
Enter DB user name : sys
Enter 'sys' password :

Configuration Validation: Success

Running rollback prerequisite checks for patch(es) "1111143,1111140" and
Oracle Home "/u01/yourinst/ap_omshome"...
Sub-patch(es) "1111143,1111140" are successfully analyzed for Oracle Home
"/u01/yourinst/ap_omshome"

Running rollback prerequisite checks for patch(es) "1111142" and Oracle Home
"/u01/yourinst/ap_extomshome"...
Sub-patch(es) "1111142" are successfully analyzed for Oracle Home "/u01/
yourinst/ap_extomshome"

Complete Summary
=====

All log file names referenced below can be accessed from the directory "/u01/
yourinst/ap_omshome/cfgtoollogs/omspatcher/
2024-12-02_12-30-09PM_SystemPatch_1111112_1"

Prerequisites analysis summary:
-----

The following sub-patch(es) are rollbackable:

           Featureset           Sub-
patches          -----          -
-----
    oracle.sysman.top.oms    1111143,1111140
1111143,1111140_opatch2024-12-02_12-31-11PM_2.log
    oracle.sysman.top.zdt        1111142
1111142_opatch2024-12-02_12-31-36PM_3.log

Log file location: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/
SystemPatch/omspatcher_2024-12-02_12-30-09PM_analyze.log

OMSPatcher succeeded.

```

Note

Once the analysis finishes, you can refer to the OMSPatcher log to see what steps would be executed by OMSPatcher in non -analyze mode. The log file contains references to the HTML and text output file HTML containing detailed steps.

Running `omspatcher apply`

Once you have downloaded the patch, see the patch README for explicit patch details and instructions on applying the patch. You can find the README at the following location

<System patch location>/README.txt (or) README.html

As you step through the patching operations in the README, running `omspatcher apply` (depending on the configuration that is patched, primary or standby) will generate a custom, environment-specific version of the README for patching operations for the primary site multi-OMS or standby site OMS systems. For a primary site single OMS system, running `omspatcher apply` will perform patching and deployment operations.

On your local OMS instance, run the following command from the top level System patch directory:

```
omspatcher apply <patch>
```

Note

Unlike `omspatcher analyze`, you should not run `omspatcher apply` on every OMS instance. OMSPatcher will either execute all patching and deployment operations, or will generate environment-specific steps that include complete configuration aspects of the System.

The primary OMS is patched using the `omspatcher apply` command. Upon completing the primary OMS patching, the OMSPatcher utility will submit a job to patch additional OMS instances. The job name will appear in the terminal from which the OMSPatcher utility is executed on the primary OMS server. The status of the multi-OMS patching job can be verified through the Enterprise Manager console or via `emcli` command.

There are two ways in which patches are applied on a multiple OMS setup.

- Automated: A job is automatically submitted that deploys the patches on each additional OMS.
- Manual: OMSPatcher provides auto-generated bash scripts that can be run on all the OMSes except the primary OMS. (UNIX and Windows based systems).

Applying a System Patch

If you want to apply a System Patch that is available on top of Enterprise Manager 24ai Release 1 release on an Oracle Home, perform the following steps:

Note

Since `omspatcher` is located in '`$ORACLE_HOME/OMSPatcher`', ensure that the directory is included in the path before running the commands.

1. Execute OMSPatcher for the System Patch.

Example:

```
$omspatcher apply /tmp/1111112
OMSPatcher Automation Tool
Copyright (c) 2024, Oracle Corporation. All rights reserved.
```

```
OMSPatcher version : 13.9.24.1.0
OUI version       : 13.9.4.0.0
```

```

Running from      : $ORACLE_HOME
Log file location : $ORACLE_HOME/cfgtoollogs/omspatcher/
opatch2024-11-26_08-08-07AM_1.log

OMSPatcher log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/
1111112/omspatcher_2024-11-26_08-08-22AM_apply.log

Please enter OMS weblogic admin server URL(t3s://
shortterm.emdev.example.com:7102):>
Please enter OMS weblogic admin server username(weblogic):>
Please enter OMS weblogic admin server password:>

Enter DB user name : sys
Enter 'sys' password :
Checking if current repository database is a supported version
Current repository database version is supported

Prereq "checkComponents" for patch 1111140 passed.

Prereq "checkComponents" for patch 1111143 passed.

Prereq "checkComponents" for patch 1111142 passed.
Configuration Validation: Success

Running apply prerequisite checks for sub-patch(es) "1111140,1111143" and
Oracle Home "/u01/yourinst/ap_omshome"...
Sub-patch(es) "1111140,1111143" are successfully analyzed for Oracle Home
"/u01/yourinst/ap_omshome"

Running apply prerequisite checks for sub-patch(es) "1111142" and Oracle
Home "/u01/yourinst/ap_extomshome"...
Sub-patch(es) "1111142" are successfully analyzed for Oracle Home "/u01/
yourinst/ap_extomshome"

To continue, OMSPatcher will do the following:
[Patch and deploy artifacts] : Apply sub-patch(es) [ 1111140 1111143
1111142 ]
                                Apply sub-patch(es) [ 1111140 1111143
1111142 ]
                                Apply RCU artifact with patch "/u01/
yourinst/ap_extomshome/.omspatcher_storage/1111142_Nov_13_2024_14_35_35/
original_patch";
                                Apply RCU artifact with patch "/u01/
yourinst/ap_omshome/.omspatcher_storage/1111143_Nov_12_2024_07_20_06/
original_patch";
                                Register MRS artifact "swlib";
                                Register MRS artifact "eventsaux";
                                Register MRS artifact
"eventSpecificCustmzn";
                                Register MRS artifact "compression";
                                Register MRS artifact "oobrules";
                                Register MRS artifact "targetType";
                                Register MRS artifact "storeTargetType";

```

```
Register MRS artifact "jobTypes";
Register MRS artifact
"default_collection";

Register MRS artifact "omsPropertyDef";
Register MRS artifact "runbooks";
Register MRS artifact "TargetPrivilege"

Do you want to proceed? [y|n]
Could not recognize input. Please re-enter.
y
User Responded with: Y
Stopping all the services on primary OMS.....
Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/
2024-11-26_08-33-29AM_SystemPatch_1111112_9/
stop_oms_all_2024-11-26_08-33-29AM.log

Stopping the Central agent .....

Starting the ADMIN .....
Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/
2024-11-26_08-33-51AM_SystemPatch_1111112_11/
start_admin_2024-11-26_08-33-51AM.log

Configure API Gateway .....
Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/
2024-11-26_08-35-14AM_SystemPatch_1111112_12/
config_apigateway_2024-11-26_08-35-14AM.log

Applying sub-patch(es) "1111140,1111143"
Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/patch/
opatch2024-11-26_08-35-19AM_6.log

Applying sub-patch(es) "1111142"
Please monitor log file: /u01/yourinst/ap_extomshome/cfgtoollogs/patch/
opatch2024-11-26_08-37-23AM_7.log

Registering the start OP .....

DB user 'sys' is allowed to perform startOP patching operation.
Update the patching flag .....

Updating repository with RCU reference file "/u01/yourinst/
ap_extomshome/.omspatcher_storage/1111142_Nov_13_2024_14_35_35/
original_patch"

Updating repository with RCU reference file "/u01/yourinst/
ap_omshome/.omspatcher_storage/1111143_Nov_12_2024_07_20_06/original_patch"

Registering service "swlib" with register file "/u01/yourinst/ap_omshome/
sysman/swlib/metadata/xml" for plugin id as "core"...
Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/
2024-11-26_08-35-14AM_SystemPatch_1111112_12/
```

emctl_register_swlib_2024-11-26_08-38-13AM.log

Registering service "eventsaux" with register file "/u01/yourinst/ap_omshome/sysman/metadata/events/auxiliary/sla_alert_aux.xml" for plugin id as "core"...

Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/2024-11-26_08-35-14AM_SystemPatch_1111112_12/

emctl_register_eventsaux_2024-11-26_08-39-12AM.log

Registering service "eventSpecificCustmzn" with register file "/u01/yourinst/ap_omshome/sysman/metadata/events/custmzn/sla_alert_cust.xml" for plugin id as "core"...

Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/2024-11-26_08-35-14AM_SystemPatch_1111112_12/

emctl_register_eventSpecificCustmzn_2024-11-26_08-39-16AM.log

Registering service "compression" with register file "/u01/yourinst/ap_omshome/sysman/metadata/events/compression/UPDATED_all_target_mce.xml" for plugin id as "core"...

Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/2024-11-26_08-35-14AM_SystemPatch_1111112_12/

emctl_register_compression_2024-11-26_08-39-20AM.log

Registering service "oobrules" with register file "/u01/yourinst/ap_omshome/sysman/metadata/events/oobrules/metric_alert_copy.xml" for plugin id as "core"...

Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/2024-11-26_08-35-14AM_SystemPatch_1111112_12/

emctl_register_oobrules_2024-11-26_08-39-24AM.log

Registering service "targetType" with register file "/u01/yourinst/ap_omshome/sysman/metadata/targetType/demo_vlm.xml" for plugin id as "core"...

Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/2024-11-26_08-35-14AM_SystemPatch_1111112_12/

emctl_register_targetType_2024-11-26_08-39-28AM.log

Registering service "storeTargetType" with register file "/u01/yourinst/ap_omshome/sysman/metadata/targetType/demo_v0m.xml" for plugin id as "core"...

Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/2024-11-26_08-35-14AM_SystemPatch_1111112_12/

emctl_register_storeTargetType_2024-11-26_08-39-33AM.log

Registering service "jobTypes" with register file "/u01/yourinst/ap_omshome/test/src/emdrep/jobs/systemtest/OSCommandNzdtTest2.xml" for plugin id as "core"...

Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/2024-11-26_08-35-14AM_SystemPatch_1111112_12/

emctl_register_jobTypes_2024-11-26_08-39-37AM.log

Registering service "default_collection" with register file "/u01/yourinst/ap_omshome/sysman/metadata/default_collection/demo_v0c.xml" for plugin id as "core"...

Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/2024-11-26_08-35-14AM_SystemPatch_1111112_12/

emctl_register_default_collection_2024-11-26_08-39-42AM.log

Registering service "omsPropertyDef" with register file "/u01/yourinst/ap_omshome/sysman/metadata/omsProperties/definition/omsprop_def_onlin_mrs.xml" for plugin id as "core"...

Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/2024-11-26_08-35-14AM_SystemPatch_1111112_12/

emctl_register_omsPropertyDef_2024-11-26_08-39-46AM.log

Registering service "runbooks" with register file "/u01/yourinst/ap_omshome/sysman/test/src/emdrep/test_plugin/OOBRunbook/plugin_dist/oms/metadata/runbooks/runbook_oob_plugin_online.xml" for plugin id as "core"...

Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/2024-11-26_08-35-14AM_SystemPatch_1111112_12/

emctl_register_runbooks_2024-11-26_08-39-50AM.log

Registering service "TargetPrivilege" with register file "/u01/yourinst/ap_omshome/plugins/oracle.sysman.vi.oms.plugin_24.1.1.0.0/metadata/security/TargetPrivilege/sample_targetpriv_oracle_nimbula_site_down1_zdt.xml" for plugin id as "oracle.sysman.vi"...

Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/2024-11-26_08-35-14AM_SystemPatch_1111112_12/

emctl_register_TargetPrivilege_2024-11-26_08-39-55AM.log

Starting the central agent

Resetting the patching flag

Resetting the job queue process

The job_queue_processes parameter is set to 0 in the repository database. Resetting the job_queue_processes parameter to default value 50 in the repository database to start the OMS. If 50 is not your default value for the job_queue_processes parameter, you should reset it to the preferred value post OMS patching.

Registering the end OP

DB user 'sys' is allowed to perform endOP patching operation.

Starting the oms

Please monitor log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/2024-11-26_08-40-24AM_SystemPatch_1111112_36/

start_oms_2024-11-26_08-40-24AM.log

Complete Summary

=====

All log file names referenced below can be accessed from the directory
"/u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/
2024-11-26_08-40-24AM_SystemPatch_111112_36"

Patching summary:

Binaries of the following sub-patch(es) have been applied successfully:

patches	Featureset	Sub-	Log file
-----	-----		-----
oracle.sysman.top.zdt_24.1.0.0.0		1111142	
1111142_opatch2024-11-26_08-37-23AM_7.log			
oracle.sysman.top.oms_24.1.0.0.0		1111140,1111143	
1111140,1111143_opatch2024-11-26_08-35-19AM_6.log			

Deployment summary:

The following artifact(s) have been successfully deployed:

Artifacts	Log file
-----	-----
SQL	
rcu_applypatch_original_patch_2024-11-26_08-37-43AM.log	
SQL	
rcu_applypatch_original_patch_2024-11-26_08-37-59AM.log	
MRS-swlib	
emctl_register_swlib_2024-11-26_08-38-13AM.log	
MRS-eventsaux	
emctl_register_eventsaux_2024-11-26_08-39-12AM.log	
MRS-eventSpecificCustmzn	
emctl_register_eventSpecificCustmzn_2024-11-26_08-39-16AM.log	
MRS-compression	
emctl_register_compression_2024-11-26_08-39-20AM.log	
MRS-oobrules	
emctl_register_oobrules_2024-11-26_08-39-24AM.log	
MRS-targetType	
emctl_register_targetType_2024-11-26_08-39-28AM.log	
MRS-storeTargetType	
emctl_register_storeTargetType_2024-11-26_08-39-33AM.log	
MRS-jobTypes	
emctl_register_jobTypes_2024-11-26_08-39-37AM.log	
MRS-default_collection	
emctl_register_default_collection_2024-11-26_08-39-42AM.log	
MRS-omsPropertyDef	
emctl_register_omsPropertyDef_2024-11-26_08-39-46AM.log	
MRS-runbooks	
emctl_register_runbooks_2024-11-26_08-39-50AM.log	

```
MRS-TargetPrivilege
emctl_register_TargetPrivilege_2024-11-26_08-39-55AM.log
```

```
Log file location: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/1111112/
omspatcher_2024-11-26_08-08-22AM_apply.log
```

OMSPatcher succeeded.

2. Run `omspatcher lspatches` command to list all the sub-patches applied in Step 1.

Syntax: `omspatcher lspatches | grep 1111112`

Example:

```
$omspatcher lspatches | grep 1111112
oracle.sysman.top.oms/24.1.0.0.0          Core
1111112          1111143          Oracle Enterprise Manager 24 C
Platform Update Test patch for Oracle Management Service
oracle.sysman.top.zdt/24.1.0.0.0          Core
1111112          1111142          Oracle Enterprise Manager 24c Test
patch for OracleZDT HOME
oracle.sysman.vi.oms.plugin/24.1.1.0.0    Plugin
1111112          1111140          Oracle Enterprise Manager for 24.1
for Oracle Management Service test patch
```

Running `omspatcher rollback`

See the patch README for explicit patch details and instructions on deinstalling the patch. You can find the README at the following location

```
<System patch location>/README.txt (or) README.html
```

As you step through the patch deinstallation operations in the README, running `omspatcher rollback` (depending on the configuration that is patched, primary or standby) will generate a custom, environment-specific version of the README for patching operations for the primary site multi-OMS or standby site OMS systems. For a primary site single OMS system, running `omspatcher rollback` will perform the deinstallation operations.

On your local OMS instance, run the following command from the top level System patch directory:

```
omspatcher rollback -systemid <system_patch_id>
```

Example:

```
$omspatcher rollback -systemid 1111112 -analyze
OMSPatcher Automation Tool
Copyright (c) 2024, Oracle Corporation. All rights reserved.
```

```
OMSPatcher version : 13.9.24.1.0
OUI version        : 13.9.4.0.0
Running from       : $ORACLE_HOME
Log file location  : $ORACLE_HOME/cfgtoollogs/omspatcher/
opatch2024-12-02_12-30-09PM_1.log
```

OMSPatcher log file: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/
SystemPatch/omspatcher_2024-12-02_12-30-09PM_analyze.log

Deobfuscating the related patch content in /u01/yourinst/ap_omshome.....
Deobfuscating the related patch content in /u01/yourinst/
ap_extomshome.....
Please enter OMS weblogic admin server URL(t3s://
shortterm.emdev.example.com:7102):>
Please enter OMS weblogic admin server username(weblogic):>
Please enter OMS weblogic admin server password:>
Enter DB user name : sys
Enter 'sys' password :

Configuration Validation: Success

Running rollback prerequisite checks for patch(es) "1111143,1111140" and
Oracle Home "/u01/yourinst/ap_omshome"...
Sub-patch(es) "1111143,1111140" are successfully analyzed for Oracle Home
"/u01/yourinst/ap_omshome"

Running rollback prerequisite checks for patch(es) "1111142" and Oracle Home
"/u01/yourinst/ap_extomshome"...
Sub-patch(es) "1111142" are successfully analyzed for Oracle Home "/u01/
yourinst/ap_extomshome"

Complete Summary
=====

All log file names referenced below can be accessed from the directory "/u01/
yourinst/ap_omshome/cfgtoollogs/omspatcher/
2024-12-02_12-30-09PM_SystemPatch_1111112_1"

Prerequisites analysis summary:

The following sub-patch(es) are rollbackable:

patches	Featureset	Sub-	Log file
-----	-----		-----
oracle.sysman.top.oms	1111143,1111140		
1111143,1111140_opatch2024-12-02_12-31-11PM_2.log			
oracle.sysman.top.zdt	1111142		
1111142_opatch2024-12-02_12-31-36PM_3.log			

Log file location: /u01/yourinst/ap_omshome/cfgtoollogs/omspatcher/
SystemPatch/omspatcher_2024-12-02_12-30-09PM_analyze.log

OMSPatcher succeeded.

Note

- Unlike `omspatcher analyze`, you should not execute the `omspatcher rollback` command on every OMS instance. OMSPatcher will either execute all patching and deployment operations, or will generate environment-specific steps that include complete configuration aspects of the System.

For a multi-OMS systems, OMSPatcher generates scripts for execution, one per OMS instance. Follow the instructions given by `omspatcher` to find those scripts. The administrators must execute these instructions to patch the various OMSes.

There are two ways in which patches are applied on a multiple OMS setup.

- Automated: A job is automatically submitted that deploys the patches on each OMS.
- Manual: OMSPatcher provides auto-generated scripts (one per OMS instance). The administrator needs to follow the steps given by OMSPatcher.

Running `omspatcher lspatches`

After the patch is applied or rolled back, you can run the `omspatcher lspatches` command to generate a comprehensive Component type - patches map of the OMS homes and installed patches.

Example:

```
$omspatcher lspatches | grep 1111112
oracle.sysman.top.oms/24.1.0.0.0          Core
1111112          1111143          Oracle Enterprise Manager 24 C
Platform Update Test patch for Oracle Management Service
oracle.sysman.top.zdt/24.1.0.0.0          Core
1111112          1111142          Oracle Enterprise Manager 24c Test
patch for OracleZDT HOME
oracle.sysman.vi.oms.plugin/24.1.1.0.0    Plugin
1111112          1111140          Oracle Enterprise Manager for 24.1
for Oracle Management Service test patch
```

Note

The last column lists all the sub-patches applied with the Release Update/Bundle Patch.

Running `omspatcher version`

To determine the version numbers of the various OMSPatcher utilities (OPlan, OsysModel) that reside on your system, you can run `omspatcher version`.

Running Zero Downtime Commands

Zero Downtime introduces the following new commands:

- `deploy`: Performs pre-downtime MRS and SQL execution.

- **update:** Perform the downtime activity and complete the patching and bring up the OMS.
- **rollback deploy:** Reverts the system back to its original state prior to a failed patching attempt.
- **status:** Returns the status of the Oracle Home patching.
- **resume:** Resumes the previous failed operation

For more information about Zero Downtime usage and commands, see [Zero Downtime Patching](#).

Patching a Standby OMS System

If you have configured a standby OMS for High Availability, refer to the chapter on "Enterprise Manager Disaster Recovery" and the appendix on Standby OMSs Using Standby WebLogic Domain" both of which can be found in the *Oracle Enterprise Manager Advanced Installation and Configuration Guide*.

Patching with Non-SYS User (Admin User)

Starting with Enterprise Manager 13c Release 5 Update 15 (13.5.0.15) or higher, you can patch the OMS using a non-SYS admin user. Oracle provides the option to perform the patching of the OMS using another user, a less-privileged Management Repository administrator user, also known as non-SYS user.

Since security is a growing concern, organizations continue to lock privileged credentials like the SYS user and Enterprise Manager administrators are having challenges in getting the SYS user account that is required for patching, plug-in deployment and install activities. Patching with the non-SYS user provides a solution with a more secure and compliant process for the patching and plug-in deployment activities.

Prerequisite:

- Patching/applying the Release Update using the non-SYS user is supported starting with Enterprise Manager 13c Release 5 Update 15 (13.5.0.15) or higher. Ensure the corresponding OMSPatcher version is downloaded from My Oracle Support as per the instructions from the patch README file.
- Once the OMSPatcher zip file is downloaded, update the OMSPatcher directory in the OMS home and ensure the version number is the same as the one updated in the patch readme file.
This step confirms that the `createLcmUserUtil` folder was created in the OMS home.
- OMSPatcher usage: You are familiar with OMSPatcher usage. Before proceeding, review [Using OMSPatcher](#).

To patch the Enterprise Manager using a non-SYS user (admin user), do the following:

1. Create the non-SYS user.

Prerequisite:

- Non-SYS user naming convention: When creating the non-SYS user, ensure that the selected name has the `SYSMAN_` prefix as part of the username.

For example: `SYSMAN_ADMIN`

- Windows Environment: Download the patch 33053642 from [My Oracle Support](#) and apply it to the Oracle home before proceeding to create the non-SYS user.

Patch 33053642 installs the Repository Create Utility (RCU) component for Windows.

You can create the new non-SYS user (admin user) in silent or interactive mode.

- **Interactive mode**

To create the non-SYS user in interactive mode, do the following:

- a. Create the non-SYS user using the `createLcmUserUtl` by running the following:

```
$ORACLE_HOME/perl/bin/perl $ORACLE_HOME/OMSPatcher/createLcmUserUtl/  
createLCMUser.pl -oh <Oracle_Home_location>
```

- All values provided interactively must be string characters.
- The value of the non-SYS user name must start with the prefix `SYSMAN_`. For example: `SYSMAN_ADMIN`.
- `$ORACLE_HOME` is the OMS home directory.
- Perl path: You need to use the Oracle_Home perl path to run the `createLcmUserUtl` utility.
- Only one non-SYS user can be created in the Enterprise Manager environment.
- Switch to SYS user is not allowed once the non-SYS user is used for the Enterprise Manager installation, patching or deploying plug-ins.

For example:

```
/u01/app/oracle/mw135/perl/bin/perl /u01/app/oracle/mw135/  
OMSPatcher/createLcmUserUtl/createLCMUser.pl -oh /u01/app/oracle/  
mw135  
Enter dbuser name : SYSMAN_ADMIN  
Enter dbuser password : Welcomepwd
```

From the above example:

- `$ORACLE_HOME` value is `/u01/app/oracle/mw135`
- `SYSMAN_ADMIN` and `Welcomepwd` are the values entered by the user interactively. `SYSMAN_ADMIN` db user is the new non-SYS user and `Welcomepwd` is the non-SYS user password.

- **Silent mode**

To create the non-SYS user in silent mode, do the following:

- a. Create a property file (text file) with the following entries:

```
sysPassword=<SYS_DATABASE_USER_PASSWORD>  
dbUser=<NON-SYS_USER> #This user will get created in the repository  
database  
dbPassword=<NON-SYS_USER_PASSWORD>
```

- All values must be string characters.
- The value of the non-SYS user must start with the prefix `SYSMAN_`. For example: `SYSMAN_ADMIN` or `SYSMAN_test`.
- Only one non-SYS user can be created in the Enterprise Manager environment.
- Switch to SYS user is not allowed once the non-SYS user is used for the Enterprise Manager installation, patching or deploying plug-ins.

For example:

```
sysPassword=Welcomepwd  
dbUser=SYSMAN_ADMIN  
dbPassword=Welcomeadminpassword
```

Save the file using any preferred name. For example: `non_sys_user.properties`.

- b. Create the non-SYS user using the `createLcmUserUtl` and the property file from step a by running the following:

```
$ORACLE_HOME/perl/bin/perl $ORACLE_HOME/OMSPatcher/createLcmUserUtl/  
createLCMUser.pl -oh <Oracle_Home_location> -silent -property_file  
<propertyfile_location>
```

For example:

```
/u01/app/oracle/mw135/perl/bin/perl /u01/app/oracle/mw135/  
OMSPatcher/createLcmUserUtl/createLCMUser.pl -oh /u01/app/oracle/  
mw135 -silent -property_file /u01/app/oracle/mw135/  
non_sys_user.properties
```

- For Windows, run the `createLcmUserUtl` utility from the `$<ORACLE_HOME>`.
- Use the `-silent` argument.
- `$ORACLE_HOME` is the OMS home directory and its value is `/u01/app/oracle/mw135`.
- You need to use the Oracle home perl path to run the `createLcmUserUtl` utility.
- Only one non-SYS user can be created in the Enterprise Manager environment.
- Switch to SYS user is not allowed once the non-SYS user is used for the Enterprise Manager installation, patching or deploying plug-ins.

Note

The non-SYS admin user can be created at any time. Once you start using the non-SYS admin user for the configuration or patching of the OMS, you cannot switch back to use SYS as an admin user to perform any of those operations. If the non-SYS admin user was created, but for some reason, you decide not to use that non-SYS user to apply the patch anymore, you can enter SYS as the admin user when applying it.

2. Apply the patch (Release Update)
Once the non-SYS user is created, you can proceed to apply the patch available from [My Oracle Support](#) which must be Enterprise Manager 13c Release 5 Update 15 (13.5.0.15) or higher version.

During the patching process, provide the non-SYS user and password details from step 1 when the Release Update (patch) requests to "Enter SYS or Non-SYS (Admin User) username" and the user password.

For information about OMSPatcher, see [Using OMSPatcher](#). For details of the apply command syntax, see [Apply](#).

Note

Silent Mode - If you are patching Enterprise Manager 13c Release 5 Update 15 (13.5.0.15) or higher, the property file must have the following entries:

```
AdminConfigFile=<String>
AdminKeyFile=<String>
Sysman_pwd=<SYS_PASSWORD>
dbUser=<NON-SYS_USER>
dbPassword=<NON-SYS_USER_PASSWORD>
```

For example:

```
AdminConfigFile=<String>
AdminKeyFile=<String>
Sysman_pwd=<SYS_PASSWORD>
dbUser=SYSMAN_ADMIN
dbPassword=Welcomadminpassword
```

Use the above property file when patching an environment that has already created the non-SYS user (instead of using SYS) as the Management Repository admin user.

OMSPatcher Command Syntax

This section provides a comprehensive listing and description of all OMSPatcher commands used to patch an OMS.

Note

OMSPatcher commands must be run from the OMS Middleware home.

OMSPatcher Commands

The OMSPatcher commands are run from the OMS Middleware home out of the OMSPatcher directory. The Middleware home must be set as \$ORACLE_HOME. In the following generic example, an OMSPatcher command is run from a Middleware home.

```
omspatcher apply <PATH_TO_PATCH_DIRECTORY>
```

where <PATH_TO_PATCH_DIRECTORY> is the full path to the System patch top level directory.

You can view online help for any command (except version) by specifying the -help option.

OMSPatcher Automation Tool

Copyright (c) 2021, Oracle Corporation. All rights reserved.

Usage: omspatcher [-help] [-analyze] [command]

```
command := apply
          rollback
          checkApplicable
          lspatches
          version
          saveConfigurationSnapshot
```

<global_arguments> := -help Displays the help message for the command.
 -analyze Print the actions, steps to be performed

without any execution.

example:

```
'omspatcher -help'
'omspatcher apply -help'
'omspatcher rollback -help'
'omspatcher checkApplicable -help'
'omspatcher lspatches -help'
'omspatcher saveConfigurationSnapshot -help'
```

OMSPatcher succeeded.

omspatcher consists of the following primary commands.

- apply
- rollback
- checkapplicable
- saveConfigurationSnapshot
- lspatches
- version

Apply

Apply a System patch to OMS instance homes. You must specify the patch location or the current directory will be used as the patch location.

Note

OMSPatcher must be run from the platform home. ORACLE_HOME environment variable must be set as the platform home or provided using the `-oh` option.

You must run the *Apply* command directly from the System patch location.

When running `omspatcher apply`, you will be prompted the following:

- WebLogic Admin Server URL of the primary OMS (or standby OMS)
- Username and Password

Silent interaction is supported by using the *silent* and *property_file* options. The *standby* option should be used if a stand by OMS system is patched. OMSPatcher can pass 'x=y' properties through the command line. See [Table 5-2](#).

Syntax

```
omspatcher apply <System patch location>
                                [-custCertPath <Path to customer optional
                                certificate>]
                                [-jre <Path to JRE>] [-nonrolling]
                                [-invPtrLoc <Path to oraInst.loc>]
                                [-property_file <Path to property file>]
                                [-analyze] [-silent] [-oh <Platform home path>]
                                [-standby]
```

Parameters

<System patch location>

Path to the location of the patch. If the patch location is not specified, then the current directory is taken as the patch location. The patch can only be a System patch.

Apply Command Options

Table 5-1 Apply

Option	Description
jre	This option tells OMSPatcher to use JRE (java) from the specified location instead of the default location under Oracle Home.
invPtrLoc	Used to locate the oraInst.loc file. Needed when the installation used the -invPtrLoc flag. This should be the path to the oraInst.loc file.
property_file	<p>The user-defined property file for OMSPatcher to use. The path to the property file should be absolute.</p> <p>The keys for 'omspatcher' are:</p> <p>'AdminConfigFile' - Encrypted file for Admin Server user of OMS instance domain.</p> <p>'AdminKeyFile' - Encrypted file for Admin Server password of OMS instance domain.</p> <p>'AdminServerURL' - Admin Server URL of OMS instance domain.</p> <p>(Example: t3s://<host address>:<port number>)</p> <p>The Key, value pair is of the format 'x=y' where 'x' is omspatcher understood key and each pair is separated by new line in the property file. This option is typically used for silent operations.</p> <p>This option is very useful for silent mode of 'omspatcher' invocation. In order to create encrypted files for WebLogic admin server username & password. Please use</p> <p>\$ORACLE_HOME/OMSPatcher/wlskeys/createkeys.sh (.cmd for windows) to get the files and load it through a custom file by 'property_file' option.</p> <p>NOTE: For Windows, please make sure that directories and files in the path are separated by "\\" in the property file.</p>
analyze	Just prints out the actions without any configuration/binary change through omspatcher.
silent	This suppresses any user-interaction.

Table 5-1 (Cont.) Apply

Option	Description
oh	The location of EM platform home. This overrides the ORACLE_HOME environment variable.
custCertPath	This option tells OMSPatcher to use the certificate from the specified location.
nonrolling	Apply and deploy the patch in non-rolling fashion, provided it is supported by the patch.
standby	This option should be used for standby OMS patching operations.

Apply Command Properties**Table 5-2 Apply Properties**

Option	Description
OMSPatcher.OMS_DISABLE_HOST_CHECK=true	Used to disable host verification check for WebLogic admin server. Please set this property to true if your OMS configuration is based on virtual host.
OMSPatcher.OMS_USER=<installed OMS user>	Use this property if OMSPatcher is not able to get the installed OMS administrator name by itself. This switch is applicable only for Windows.
OMSPatcher.OMS_SCRIPTS_DIR=<existing directory>	This switch is applicable only for UNIX systems. By providing an existing directory, the bash scripts produced by OMSPatcher for multi-OMS are copied to a newly created time stamped sub-directory under the directory specified by the administrator. This would help OMS administrator to execute the scripts from pre-determined shared location, if any, rather than manual scripts copied to each OMS box.

Rollback

Roll back sub-patches of a System patch from OMS instance home. Administrator specifies the System patch id to be rolled back. You can obtain the sub-patch IDs by running the `omspatcher lspatches` command. See ["Running omspatcher lspatches"](#).

Important: OMSPatcher must be run from the Middleware home. ORACLE_HOME environment variable must be set as platform home or provided via the `-oh` option.

When running `omspatcher rollback`, you will be prompted the following:

- WebLogic Admin Server URL of the primary OMS (or standby OMS)
- Username and Password

Silent interaction is supported by using the *silent* and *property_file* options. The *standby* option should be used if a stand by OMS system is patched. OMSPatcher can pass 'x=y' properties through the command line. See [Table 5-2](#).

Syntax

```
omspatcher rollback -systemid <System patch ID>
                    [-custCertPath <Path to customer optional certificate>]
                    [-invPtrLoc <Path to oraInst.loc>]
                    [-jre <LOC>] [-silent] [-nonrolling]
                    [-property_file <path to property file>]
                    [-analyze] [-oh <Platform home path>]
                    [-skipautopatch_addoms] [deploy]
                    [-spb_patch]
```

Parameters

System patch id for the System patch to be rolled back.

Rollback Options

Table 5-3 Rollback

Option	Description
systemid	Use omspatcher <code>lspatches</code> option to display all patch ids for both core home and plug in homes with relation to the System patch bundles. The patch ids can be only from one bundle in a session. The list is separated by commas.
invPtrLoc	Used to locate the <i>oraInst.loc</i> file. Needed when the installation used the <i>invPtrLoc</i> flag. This should be the path to the <i>oraInst.loc</i> file.
jre	This option tells omspatcher to use JRE (java) from the specified location instead of the default location under Oracle Home.
silent	This option suppresses any user-interaction.
nonrolling	Roll back and deploy the patch in non-rolling fashion, provided it is supported by the patch.
property_file	<p>The administrator defined property file for omspatcher to use. The path to the property file should be absolute.</p> <p>The keys for 'omspatcher' are:</p> <p>'AdminConfigFile' - Encrypted file for Admin Server user of OMS instance domain.</p> <p>'AdminKeyFile' - Encrypted file for Admin Server password of OMS instance domain.</p> <p>'AdminServerURL' - Admin Server URL of OMS instance domain.</p> <p>(Example: t3s://<host address>:<port number>)</p> <p>The key value pair is of the format 'x=y' where 'x' is omspatcher understood key and each pair is separated by new line in the property file. This option is typically used for silent operations.</p> <p>This option is very useful for silent mode of 'omspatcher' invocation. In order to create encrypted files for WebLogic admin server username & password, Please use <code>\$ORACLE_HOME/OMSPatcher/wlskeys/createkeys.sh</code> (command for windows) to get the files and load it through a custom file by 'property_file' option.</p> <p>NOTE: For Windows, ensure that directories and files in the path are separated by "\" in the property file.</p>
analyze	Displays out the actions without any configuration/binary change through 'omspatcher'.

Table 5-3 (Cont.) Rollback

Option	Description
custCertPath	This option tells OMSPatcher to use the certificate from the specified location.
oh	The location of EM platform home. This overrides the ORACLE_HOME environment variable.
standby	This option should be used for standby OMS patching operations.

Rollback Command Properties**Table 5-4 Rollback Properties**

Option	Description
OMSPatcher.OMS_DISABLE_HOST_CHECK=true	Used to disable host verification check for WebLogic admin server. Please set this property to true if your OMS configuration is based on virtual host.
OMSPatcher.OMS_USER=<installed OMS user>	Use this property if OMSPatcher is not able to get the installed OMS administrator name by itself. This switch is applicable only for Windows.

lspatches

Displays the list of patches applied to the OMS home. It will show the component Name/Version, Component Type, System patch, Sub-patch and patch description where patch has been applied. Please note that OMSPatcher will be used to apply only system patches. However the OMS can have one-off patches which would have already been applied at the time of the Enterprise Manager installation. OMSPatcher provides information about whether the patch is a system patch or one-off patch and, if it is the system patch, then it will also show all other patches that are part of that system patch.

Syntax

```
omspatcher lspatches [ -invPtrLoc <Path to oraInst.loc> ]
                    [-jre <LOC> ]
                    [-oh]
```

Options**Table 5-5 lspatches**

Option	Description
jre	This jre option instructs OMSPatcher to use the JRE (java) from the specified location instead of the default location under Oracle Home.
invPtrLoc	The invPtrLoc option is used to locate the Central Inventory Pointer File (oraInst.loc). Input for this option is the path to the oraInst.loc file.
oh	The location of Middleware home. This overrides the ORACLE_HOME environment variable.

version

The `version` command shows the current version number of the OPatch utility, dependent OPlan version, and the osysmodel version.

Important: OMSPatcher must be run from the Middleware home.

Syntax

```
omspatcher version [-invPtrLoc <Path to oraInst.loc>]
                  [-jre <LOC>]
                  [-oh <ORACLE_HOME>]
                  [-help] [-h]
```

Options

The following table describes the options available for the `version` command.

Table 5-6 `version` Command Options

Option	Description
-invPtrLoc	The <code>invPtrLoc</code> option is used to locate the Central Inventory Pointer File (<code>oraInst.loc</code>). Input for this option is the path to the <code>oraInst.loc</code> file.
-jre	This <code>jre</code> option instructs OMSPatcher to use the JRE (java) from the specified location instead of the default location under Oracle Home.
-oh	The <code>oh</code> option specifies the Oracle Home to work on. This takes precedence over the environment variable <code>ORACLE_HOME</code> .

checkApplicable

The `checkApplicable` command performs prerequisite binary checks on the OMS platform home and plug-in homes to determine the applicability of a System patch and/or the whether sub-patches of the System patch can be rolled back.

Syntax

```
omspatcher checkApplicable
                  [-id <singleton or System Patch ID to be rolled back>]
                  [-custCertPath <Path to customer optional certificate>]
                  [-invPtrLoc <Path to oraInst.loc>]
                  [-jre <LOC>]
                  [-ph <System patch that is to be installed>] [-silent]
```

Options

The following table describes the options available for the `checkApplicable` command.

Table 5-7 `checkApplicable` Command Options

Option	Description
id	This option can be used to specify the sub-patch IDs that are to be rolled back from the OMS platform home or plug in homes.

Table 5-7 (Cont.) checkApplicable Command Options

Option	Description
invPtrLoc	Used to locate the <code>oraInst.loc</code> file. Needed when the installation used the <code>-invPtrLoc</code> flag. This should be the path to the <code>oraInst.loc</code> file.
jre	This option tells OMSPatcher to use JRE (java) from the specified location instead of the default location under Oracle Home.
ph	This option can be used to specify the path to the patch location. The input must be a System patch location.
silent	This suppresses any user-interaction.
custCertPath	This option tells OMSPatcher to use the certificate from the specified location.

saveConfigurationSnapshot

The `saveConfigurationSnapshot` command generates configuration a snapshot for the primary OMS (along with OMS repository) and saves it to an XML file that can be read by OMSPatcher.

If file is not specified, it will be saved to a default file (`configData.xml`) at the following location

```
ORACLE_HOME/cfgtoollogs/omspatcher/sysconfig/configData.xml
```

When running the `saveConfigurationSnapshot` command, you will be prompted for the following:

- WebLogic Admin Server URL of the primary OMS
- Username and password

You can run the command in silent mode (suppress user interaction) via the *silent* and *property_file* options.

This command must be run from an OMS instance belonging to the primary OMS system. If the OMS configuration is running on a virtual host, you must set the `OMSPatcher.OMS_DISABLE_HOST_CHECK=true` option from the command line.

Syntax

```
omspatcher saveConfigurationSnapshot
  [-configFile <File to save configuration snapshot> ]
  [-oh <ORACLE_HOME> ]
  [-invPtrLoc <Path to oraInst.loc> ]
  [-jre <LOC> ]
  [-silent ]
  [-property_file <path to file> ]
```

Options

The following table describes the options available for the `version` command.

Table 5-8 saveConfigurationSnapshot Command Options

Option	Description
configFile	Enables OPatch to write the configuration for the specified product to an XML file. The XML file can only be recognized by Oracle System Model APIs and accessed through via the Enterprise Manager SDK.
oh	Specifies the Oracle home to be worked on. The Oracle Home specified takes precedence over the environment variable ORACLE_HOME.
invPtrLoc	Used to locate the oralnst.loc file. Needed when the installation used the -invPtrLoc flag. This should be the path to the oralnst.loc file.
jre	Instructs OMSPatcher to use JRE (java) from the specified location instead of the default location under Oracle Home.
silent	Suppresses any user-interaction.
property_file	<p>The user-defined property file for OMSPatcher to use. The path to the property file must be absolute.</p> <p>The keys for 'OMSPatcher' are:</p> <ul style="list-style-type: none"> AdminConfigFile - Encrypted file for Admin Server user of the GC Domain. AdminServerURL - Admin Server URL of GC Domain (Example: t3s://<host address>:<port number>) AdminKeyFile - Encrypted file for Admin Server password of the GC Domain. <p>The Key, value pair is of the format 'x=y' where 'x' is an OMSPatcher understood key and each pair is separated by newline in the property file.</p> <p>The <code>property_file</code> option is typically used when running OMSPatcher in silent mode operation (suppress user interaction)</p> <p>In order to create encrypted files for a WebLogic Admin Server username & password, run the following script:</p> <pre>\$MW_HOME/OMSPatcher/wlskeys/createKeys.sh</pre> <p>(createKeys.cmd for Windows) to obtain the files and load them through a custom file using the <code>property_file</code> option.</p> <p>NOTE: For Windows, make sure that directories, files in the path are separated by "\\" in the property file.</p>

Zero Downtime Patching

Customers use Enterprise Manager (EM) for monitoring, diagnostics, and lifecycle automation of their mission-critical databases, middleware, packaged applications, and engineered systems. Keeping current with the latest Release Update (RU) while meeting Service Level Agreements (SLA) and minimizing loss of monitoring for critical targets can be a challenge for EM administrators. To meet these challenges, you can use Zero Downtime (ZDT) patching for applying release update on EM while it is up and running, thereby ensuring that critical monitoring and alerting are available during planned maintenance window.

Patching can be a time consuming and error prone activity. Zero Downtime patching automates the tasks required for patching and reduces the risk of human error.

Zero Downtime patching allows the patching process (`deploy`) to take place while the OMS is running: There's no system downtime. Not having the OMS down for extended periods provides benefits such as continued target monitoring and critical alerting for your business-critical applications during planned maintenance.

- [Prerequisites](#)
- [Limitations](#)
- [EM Monitoring When Performing Zero Downtime Patching](#)

Prerequisites

Before running an OMSPatcher patching session, you must ensure the following configuration and inventory-based prerequisites are satisfied: Configuration-based conditions that have to be honored for OMS automation is given below.

- Repository DB should be at a minimum of version 19.22 or higher.
- The Enterprise Manager Software library must be configured.
- The Oracle WebLogic Administration Server that controls the OMS instance (currently to be patched) through a managed server must be up and running.
- Ensure that the Oracle Database, which houses the OMS Management Repository, and its listener are up and running.
- Ensure that you have the latest version of the OMSPatcher in the OMS platform home of each host.
- Ensure that you have the latest version of the OPatch in the OMS platform home of each host.
- Ensure there is a 25GB of free space available on the same file system as the OMS. This space is used for cloning the OMS home.
- The OMS Base directory should be owned by the same user as the OMS. Example:
If /u01/app/OMS is the OMS_HOME, /u01/app should be owned by the same user as the OMS.
- It is recommended to backup the repository DB during the `omspatcher update` operation where the OMS downtime is initiated. We recommend using a restore point for backing up the repository DB as this will minimize the downtime.
- Admin server password (weblogic password) and repository database `sys` user password are needed for patching.
- For OMS installed on windows, ensure that the one off patch 33053642 is applied on the OMS.
- While patching Multi OMS environment, make sure:
 - The patch is staged on a shared mount point, preferably the software library.
 - The central agents on the additional OMSes are up and running.
- Check your patch README to determine whether there are any specific prerequisites to be executed based on patch and patching methodologies.

Limitations

When running Zero Downtime patching, there are operational restrictions:

- OMS patching in parallel with two or more different patches: You should not apply any other patches on the OMS until the complete patching activity is done.
- Additional OMS deployment should not be performed during the deploy or pre-downtime activity phase. Doing so will place the system in an inconsistent state.

- Plug-in deployment or un-deployment: After the completion of the deploy phase (pre-downtime) activity, it is recommended not to perform any plug-in deployment/un-deployment until the update phase is complete.

EM Monitoring When Performing Zero Downtime Patching

Even as you are performing Zero Downtime patching, if you have at least 2 OMS instances in your Enterprise Manager system, the Zero Downtime (ZDT) Monitoring Service continues to be available to provide monitoring and alerting functionality. For more information, see [Zero Downtime Monitoring](#) in the *Enterprise Manager Monitoring Guide*.

OMSPatcher Command Updates

To support Zero Downtime patching operations, new command options have been added. In addition, updates to the existing commands have been made.

The following table lists all OMSPatcher changes to support Zero Downtime patching.

Command	Syntax	Additional Information
deploy	omspatcher deploy <patch location>	<p>Performs pre-downtime Metadata Registration Service (MRS) and SQL execution.</p> <p>Recovery Operations</p> <p>If the pre-downtime operations have failed, do one of following while the OMS is up and running</p> <ul style="list-style-type: none"> • Fix the issue by running the patching <code>resume</code> operation. [online operation] • Run pre-downtime <code>omspatcher rollback deploy</code> to restore the OMS to its previous state before patching started. [online operation] • Restore the backup. [offline operation] Note: This option should only be used as a last resort.
deploy -analyze	omspatcher deploy -analyze <patch location>	The -analyze option analyzes a patch from the location where the patch was unzipped. The command provides details on the compatibility of the patch with the OMS.

Command	Syntax	Additional Information
update	omspatcher update	<p>This command will perform the downtime activity and complete the patching and bring up the OMS.</p> <p>Recovery Method</p> <p>If there is downtime activity failure, do the following:</p> <ol style="list-style-type: none"> 1. Fix the issue and run resume. 2. Restore from the middleware home backup made in step 2 (Downtime Activity) above.
rollback deploy	omspatcher rollback deploy	<p>If the failure occurs during the pre-downtime phase, this verb allows you to revert the system back to its original state prior to the failed patching attempt.</p> <p>If you do not want to complete the patching using update after the deploy is successful, then you can run this command to go back to the previous state.</p> <p>This is an online operation.</p>
status	omspatcher status	<p>The command returns the status of the Oracle Home patching. Specifically, the following is shown:</p> <ul style="list-style-type: none"> • General information about the applied patch • State of Oracle Home whether pre-downtime is completed • Whether downtime is pending or nothing pending. • Notification in Enterprise Manager to show that pre-downtime has been done and downtime is pending
resume	omspatcher resume	<p>This command will resume the previous failed operation and is platform independent (instead of running previous resume.sh).</p>

Zero Downtime Patching Workflow

The following high-level workflow illustrate the patching process for Zero Downtime OMS patching.

Note

For specifics on command option updates for Zero Downtime patching, see [OMSPatcher Command Updates](#).

Step 1: [Analyze](#)

Step 2: [Deploy](#)

Step 3: [Update](#)

Step 4: [Verify](#)

Optional: [Rollback](#)

Step 1: Analyze

Analyze a patch from the location where the patch was unzipped to check patch compatibility with the OMS.

```
omspatcher deploy -analyze <patch location>
```

Step 2: Deploy

Run OMSPatcher in Zero Downtime mode.

```
omspatcher deploy <pl patch location>
```

Running the `deploy` command in mode will execute pre-downtime tasks.

Step 3: Update

Note

Enterprise Manager Console access will be temporarily unavailable during the update phase.
Enterprise Manager is under planned maintenance to deploy the Release Update. Monitoring, incidents, and notifications will continue to work, but access to the Console is temporarily unavailable during the update phase.

```
omspatcher update
```

1. Ensure you have backed up the middleware home (Recommended).
2. Prompt for confirmation from administrators that the database has been backed up.
3. Make sure you have available the procedure to take the database backup.

Step 4: Verify

For patch verification, see [Post-Patching Verification](#).

Optional: Rollback

Follow these steps if you want to rollback the patch that was applied.

1. Shut down the OMS.

- 2. Run the `rollback` command with the patch id.

`omspatcher rollback -systemid <patchid>`
- 3. Roll back the patch.
- 4. Bring up the OMS.

Patching Use Cases

The following use cases demonstrate OMSPatcher command usage for various patching scenarios.

Prerequisites

- Download the patch that needs to be applied. See [My Oracle Support: Searching for Patches](#).
- Make sure that the installed version of OMSPatcher and OPatch matches the version specified in the *Readme* of the patch being applied. This has to be updated in the Oracle Home.

Use Case	Single OMS	Multi-OMS
Apply patch A	<code>omspatcher deploy <patchA location></code> <code>omspatcher update</code>	Run on the Primary OMS <code>omspatcher deploy <patchA location></code> <code>omspatcher update</code> For multi-OMS environments, once the patching is completed on the primary OMS, a job will be started to patch the additional OMS.
Apply only the one-off patch without the Enterprise Manager Release Update	<code>omspatcher deploy <one-off location></code> <code>omspatcher update</code>	Run on the Primary OMS <code>omspatcher deploy <one-off location></code> <code>omspatcher update</code>

Use Case	Single OMS	Multi-OMS
Apply patch A Rollback patch A	<ol style="list-style-type: none"> 1. <code>omspatcher deploy <patchA location></code> 2. <code>omspatcher update</code> 3. <code>emctl stop oms</code> 4. <code>omspatcher rollback - systemid <systemid></code> 	<p>Run on the Primary OMS</p> <p><code>omspatcher deploy <patchA location></code> <code>omspatcher update</code></p> <p>Once patchA jobs have finished execution on the additional OMS, do the following:</p> <ol style="list-style-type: none"> 1. Run the following on the Primary OMS and additional OMS: <code>emctl stop oms</code> 2. Run the following on the Primary OMS: <code>omspatcher rollback - systemid <systemid></code>
Weblogic/stack patches	<ol style="list-style-type: none"> 1. Update Opatch to the latest version. For more information about OPatch, see Introduction to OPatch and Patching. 2. <code>emctl stop oms</code> 3. <code>opatch napply <patch location></code> 	<ol style="list-style-type: none"> 1. Place the <code>opatch.omspatcher</code> file and RUs in the <code>swlib</code> location for the additional OMS job to pick it up. 2. Run the following on the Primary OMS and additional OMS: <code>emctl stop oms</code> 3. Run the following on the Primary OMS: <code>opatch napply <patch location></code> 4. Run the following on all additional OMS instances: <code>opatch napply <patch location></code>

Use Case	Single OMS	Multi-OMS
Weblogic/stack patches with Enterprise Manager Release Update	<p>Suggestion: Consume the Release Update in non-ZDT mode as one downtime is required for Weblogic/stack patches.</p> <ol style="list-style-type: none"> 1. Update Opatch and OMSPatcher to the latest version. 2. <code>emctl stop oms</code> 3. <code>opatch napply <patch location></code> 4. <code>omspatcher apply <RU location>.apply</code> 5. <code>emctl start oms</code> 	<p>Suggestion: Consume the RU in non-zero downtime mode as one downtime is required for Weblogic/stack patches.</p> <ol style="list-style-type: none"> 1. Place the <code>opatch.omspatcher</code> file and RUs in the <code>swlib</code> location for the additional OMS job to pick it up. 2. Run the following on the Primary OMS and additional OMS: <code>emctl stop oms</code> 3. Run the following on the Primary OMS: <code>opatch napply <patch location></code> 4. Run the following on all additional OMSSes: <code>opatch napply <patch location></code> 5. <code>omspatcher apply <RU location></code>
		<p>Note</p> <p>Running <code>omspatcher apply</code> does not apply the patch on multi-OMS setups. Instead, it will generate the necessary scripts that need to be run on each OMS.</p>
		<ol style="list-style-type: none"> 6. <code>emctl start oms</code>

Applying MRS Artifacts

For Zero Downtime patching, most of the MRS artifacts are applied during the `deploy` phase.

The following workflow illustrates where in the patching process MRS artifacts need to be applied. As mentioned earlier, there are two patching phases corresponding to the OMS state:

- Deploy
- Update

The following table shows the tasks to be performed during each phase.

Deploy	Update
<ol style="list-style-type: none"> 1. Create clone 2. Create new edition 3. Apply bits 4. Apply sqls 5. Apply MRS 	<p>Divide the OMSes into 2 batches.</p> <ol style="list-style-type: none"> 1. Shut down all the OMSes from batch #1 2. Apply bit-only 3. Submit the job on the add OMSes from batch #1 4. Bring down the add OMSes from batch #2 5. Switch the edition 6. Apply the MRS artifacts 7. Bring up the primary OMS and then add OMSes from batch #1 8. Jobs will be submitted to apply the patch on additional OMSes from batch #2

Post-Patching Verification

After completing the Zero Downtime patching, do the following for verification:

1. Confirm that all OMSes are up and running.
2. Check whether the patch is available in all OMSes.

Holistic Patching

Holistic patching offers a comprehensive solution for efficiently managing security updates for Enterprise Manager infrastructure.

Holistic patching is used for applying the Enterprise Manager quarterly Critical Patch Update (CPU patches). The use of a single patch minimizes downtime while addressing vulnerabilities and reducing the risk of security breaches.

To patch the Enterprise Manager using holistic patching, refer to the README file.

Holistic patching is facilitated by the Stack Patch Bundle.

Stack Patch Bundle (SPB)

- It's a big stack patch bundle that consolidates critical components in Enterprise Manager such as OHS, OPSS, WLS and JDK, and in consequence reducing security risks.
- The use of SPB simplifies the application of CPU patches.
- SPB is orchestrated through OMSPatcher utility.
- The EM administrator can download a single holistic patch from My Oracle Support for Enterprise Manager quarterly CPU cycle.
- SPB enhances system security since it ensures the JDK inside the OMS home is updated to comply with the latest certified version.

When using holistic patching, applying CPU patches are easier to perform by following the below steps:

- Download single holistic patch from My Oracle Support for quarterly CPU cycle.

- Apply SPB through OMSPatcher to reduce security risks. During this process, the JDK inside the OMS home will get updated to comply with the latest certified version.

Benefits of holistic patching:

- Reduces the maintenance window
 - Single downtime window to apply holistic patch and release updates.
 - System and environment prechecks are performed once hence reducing the overall apply time.

Holistic Patching Orchestration using OMSPatcher

To apply holistic patch and release updates to the OMS, you only need to use the *OMSPatcher* utility.

The `omspatcher apply` command upgrades the `opatch` to the required version and updates the JDK inside the OMS home.

New OMSPatcher Commands Available to Deploy Holistic Patching

Holistic patching, facilitated by the Stack Patch Bundle, is orchestrated through the *OMSPatcher* utility and new parameters are added to the *OMSPatcher* to execute SPB patch.

The `-spb_patch` new parameter is for holistic patching and it indicates that the `omspatcher apply` operation is specifically for holistic stack patch bundle.

Note

In the case of multi-OMS patching, additional OMS patching scripts are generated at the end of primary OMS patching. You need to copy the scripts to the additional OMS nodes and execute the scripts manually to complete the patching process.

- Analyze holistic patch
It conducts thorough analysis of holistic patch to identify any potential conflicts and ensure all prerequisite checks are met before deployment. If there are patch conflicts, the command will return with the conflicting patch information. Oracle recommends to analyze the holistic patch before applying it.

```
omspatcher apply <patch location> -spb_patch -analyze
```

- Apply holistic patch
It applies the holistic patch. As part of the process, the OMSPatcher first validates the JDK update. The OMSPatcher compares the JDK update version inside the OMS home with the version included in the holistic patch. If the JDK update version inside the OMS home is outdated, the apply process automatically updates the JDK.

Patches are also applied to various components such as OHS, OPSS, OSS, WLS, ADR, ADF, etc., within the OMS home. Upon completion of the apply phase, the primary OMS is started.

```
omspatcher apply <patch location> -spb_patch
```

- Apply holistic patch in silent mode

```
omspatcher apply <patch location> -spb_patch -silent
```

- Apply holistic patch and JDK update

```
omspatcher apply <patch location> -spb_patch -jdk_update <jdk location>
```

Note

For OMS on AIX, the `-jdk_update` parameter needs to be explicitly passed to the `omspatcher apply` command.

For other Unix platforms (LinuxX64, Solaris, etc), there's no need to pass the `-jdk_update` parameter since the JDK will get updated as part of apply command.

- Rollback holistic patch

```
omspatcher rollback -id <patch id list> -spb_patch
```

To verify if the patches were applied inside the OMS home, use the `omspatcher lspatches` command and check if the patch is registered in the inventory.

Troubleshooting

This chapter describes common OMSPatcher problems that may occur during patching operations or the analyze phase.

This chapter covers the following:

- [OMSPatcher Troubleshooting](#)
- [OMSPatcher Log Management](#)
- [Logs for Oracle Support](#)
- [OMSPatcher: Cases Analysis, Error Codes, and Remedies/Suggestions](#)
- [OMSPatcher: External Utilities Error Codes](#)
- [Special Error Cases for OMSPatcher OMS Automation](#)

OMSPatcher Troubleshooting

In order for OMSPatcher to fully automate the patching process, it accesses various tools/utilities to carry out different patching tasks in their respective phases. The primary tools/utilities outside of OMSPatcher are:

- `emctl stop oms`
- `emctl start oms`

These tools/utilities are accessed during the patching process. Note that failure during invocation of these utilities can also happen and the errors & remedies for those commands are not handled in this document. They need to be followed up with Oracle Support for details. However, OMSPatcher will trap errors from these commands output, push it to appropriate logs and announce it to the administrator and finally to support.

Apart from the above external tools/utilities, OMSPatcher uses the following internal utilities to do binary patching operations. They have separated log files generated by OMSPatcher. The internal utilities are patch binary prerequisite checks and patch binary apply, rollback operations.

OMSPatcher Log Management

This section refers to the information through logs published by OMSPatcher as part of its patching operations. This knowledge is needed for the administrator to obtain the appropriate logs from right area to troubleshoot and inform Oracle Support for further analysis. The following annotated example shows OMSPatcher apply output that displays the various log files that are created when running OMSPatcher.

Sample OMSPatcher apply Output

```
$ORACLE_HOME/OMSPatcher/omspatcher apply -bitonly
OMSPatcher Automation Tool
Copyright (c) 2024, Oracle Corporation. All rights reserved.
```

```
OMSPatcher version : 13.9.24.1.0
OUI version        : 13.9.4.0.0
Running from       : $ORACLE_HOME
Log file location  : $ORACLE_HOME/cfgtoollogs/omspatcher/
opatch2024-11-19_16-23-37PM_1.log
```

```
OMSPatcher log file: $ORACLE_HOME/cfgtoollogs/omspatcher/1111112/
omspatcher_2024-11-19_16-23-50PM_apply.log
```

```
WARNING: OMSPatcher has been invoked with bitonly option but the System patch
provided has deployment metadata.
Invocation in bitonly mode will prevent OMSPatcher from deploying artifacts.
```

```
Do you want to proceed? [y|n]
Y
User Responded with: Y
```

```
Prereq "checkComponents" for patch 1111140 passed.
```

```
Prereq "checkComponents" for patch 1111143 passed.
```

```
Prereq "checkComponents" for patch 1111142 passed.
```

```
Running apply prerequisite checks for sub-patch(es) "1111140,1111143" and
Oracle Home "$ORACLE_HOME"...
Sub-patch(es) "1111140,1111143" are successfully analyzed for Oracle Home
"$ORACLE_HOME"
```

```
Running apply prerequisite checks for sub-patch(es) "1111142" and Oracle Home
"$ORACLE_HOME"...
Sub-patch(es) "1111142" are successfully analyzed for Oracle Home
"$ORACLE_HOME"
```

```
To continue, OMSPatcher will do the following:
[Patch and deploy artifacts] :
Do you want to proceed? [y|n]
Y
User Responded with: Y
```

```
Applying sub-patch(es) "1111140,1111143"
```

Please monitor log file: \$ORACLE_HOME/cfgtoollogs/opatch/
opatch2024-11-19_16-26-37PM_3.log

Applying sub-patch(es) "1111142"
Please monitor log file: \$ORACLE_HOME/cfgtoollogs/opatch/
opatch2024-11-19_16-28-19PM_4.log

Starting the ADMIN
Please monitor log file: \$ORACLE_HOME/cfgtoollogs/omspatcher/
2024-11-19_16-23-37PM_SystemPatch_1111112_1/
start_admin_2024-11-19_16-28-25PM.log

Configure API Gateway
Please monitor log file: \$ORACLE_HOME/cfgtoollogs/omspatcher/
2024-11-19_16-23-37PM_SystemPatch_1111112_1/
config_apigateway_2024-11-19_16-28-35PM.log

Complete Summary
=====

All log file names referenced below can be accessed from the directory
"\$ORACLE_HOME/cfgtoollogs/omspatcher/
2024-11-19_16-23-37PM_SystemPatch_1111112_1"

Patching summary:

The following sub-patch(es) are applicable:

patches	Featureset	Sub-	Log file
-----	-----		-----
oracle.sysman.top.oms	1111140,1111143		
1111140,1111143_opatch2024-11-19_16-40-51PM_2.log			
oracle.sysman.top.zdt	1111142		
1111142_opatch2024-11-19_16-42-01PM_2.log			

--
The following warnings have occurred during OPatch execution:
1) OMSPatcher has been invoked with bitonly option but the System patch
provided has deployment metadata.
Invocation in bitonly mode will prevent OMSPatcher from deploying artifacts.

--

Log file location: \$ORACLE_HOME/cfgtoollogs/omspatcher/1111112/
omspatcher_2024-11-19_16-23-50PM_apply.log

OMSPatcher succeeded.

Log output to a consolidated directory

As shown in the example above, there is a reference to pushing all logs to a consolidated log directory. The following line in the trace example shows this consolidation log directory.

```
...
All log file names referenced below can be accessed from the directory
"$ORACLE_HOME/cfgtoollogs/omspatcher/
2023-02-15_11-50-27AM_SystemPatch_111112_1"
...
```

This consolidated log directory contains the following files (here with reference to the example for rollback).

```
$ ls -l $ORACLE_HOME/cfgtoollogs/omspatcher/
2023-02-15_11-50-27AM_SystemPatch_111112_1

-rw-r--r-- 1 myadmin g900 39975 May 30 03:24
1111126,1111137,1111155_opatch2018-05-30_03-23-31AM_3.log
-rw-r--r-- 1 myadmin g900 13219 May 30 03:24
1111126,1111155,1111137_opatch2018-05-30_03-22-01AM_2.log
-rw-r--r-- 1 myadmin g900 120 May 30 03:22
AdminServerStatusPrerequisites_2018-05-30_03-22-01AM.log
-rw-r--r-- 1 myadmin g900 66 May 30 03:22
RepositoryStatusPrerequisites_2018-05-30_03-22-01AM.log
-rw-r--r-- 1 myadmin g900 71 May 30 03:22
Swlib_Prerequisite_2018-05-30_03-22-01AM.log
-rw-r--r-- 1 myadmin g900 456 May 30 03:24
emctl_register_VCPUUtilization_2018-05-30_03-24-28AM.log
-rw-r--r-- 1 myadmin g900 451 May 30 03:24
emctl_register_eventsaux_2018-05-30_03-24-20AM.log
-rw-r--r-- 1 myadmin g900 418 May 30 03:24
emctl_register_mpcui_2018-05-30_03-24-34AM.log
-rw-r--r-- 1 myadmin g900 418 May 30 03:24
emctl_register_mpcui_2018-05-30_03-24-40AM.log
-rw-r--r-- 1 myadmin g900 12574 May 30 03:24 opatch2018-05-30_03-21-43AM_1.log
-rw-r--r-- 1 myadmin g900 3938 May 30 03:24 temp_apply_automation.xml
-rw-r--r-- 1 myadmin g900 3149 May 30 03:24 temp_rollback_automation.xml
```

All individual log files of all invocation commands are finally copied to a consolidated place as highlighted above. Each command naming convention is self-explanatory and it indicates the actual operations being performed in automation. The *omspatcher* log file will refer the individual log files so that administrator can easily connect to individual files to refer to any failure.

Logs for Oracle Support

If the administrator wants to contact Oracle Support, the administrator must provide the following references to Support.

- Administrator interface trace(s).
- Consolidated log directory as zip
- OPatch log file
- OMSPatcher log file
- Output of `omspatcher lspatches` command on all OMS instance homes.

OMSPatcher: Cases Analysis, Error Codes, and Remedies/Suggestions

Refer to the following table for common OMSPatcher error codes.

Table 5-9 OMSPatcher Error Codes

Error Code	Description	Remedy/Suggestion
231	Wrong Oracle WebLogic Administration Server URL and/or invalid credentials	Correct the interview inputs and run OMSPatcher again.
234	Malformed Oracle WebLogic Administration Server URL	If the Oracle WebLogic Administration Server URL is already defaulted (value given), type <enter>. If it is not given, construct the Oracle WebLogic Administration Server URL as t3s://<WebLogic Administration Server host address>:<WebLogic Administration Server port>.of the domain that controls the managed server on which the OMS is deployed.
235	Unable to connect to OMS repository	Check the OMS repository connectivity for SYSMAN administrator and run OMSPatcher again.
236	OUI central inventory read issue	Check if the OUI inventory is locked by some other processes. Check if OUI inventory is readable.
238	Patch binary prerequisite checks failure	Check OMSPatcher, OPatch, patch binary prerequisite log files for more details on the errors. If not resolved, contact Oracle Support.

Table 5-9 (Cont.) OMSPatcher Error Codes

Error Code	Description	Remedy/Suggestion
240 - 251	Binary updates (or) deployment failure	<ul style="list-style-type: none"> This is a case for single OMS system. Patching steps are decided by OMSPatcher but it failed to execute steps. OMSPatcher will print the failed executed step and the remaining steps to be executed for completion of patching operations. Administrator needs to contact Oracle support with logs, resolve why it failed and then must execute manually the failed step and steps referred by OMSPatcher (in OMSPatcher log file) to complete operations. In case of multi OMS (or) stand by OMS patching operations, failure of individual commands that got executed through text/html output must be brought to support notice for further diagnosis. After the failure condition is resolved, administrator needs to execute the failed steps and further steps mentioned in HTML (or) text output to complete the patching operations.
233	Software library not configured OMS repository connectivity not achieved. (post successful check of the same during credential inputs Oracle WebLogic Administration Server not reachable (post successful check of the same during credential inputs)	Check the OMSPatcher log file for the failure.

OMSPatcher: External Utilities Error Codes

The following table lists exit codes for external utilities that OMSPatcher uses for life cycle and deployment. If the deployment (or) life cycle fails through OMSPatcher, the administrator can search individual log files for the error messages shown in the *Error Message/Recommendation* column.

Table 5-10 OMSPatcher External Utilities Error Codes

Exit Code	Error Message / Recommendation
34	Displays the usage of the command.
35	Unable to read password! Exiting...
36	Unable to get a connection to the repository! Exiting...
37	The Plug-in is not deployed on this Management Server. The plug-in has to be deployed first to register metadata for that plug-in.

Table 5-10 (Cont.) OMSPatcher External Utilities Error Codes

Exit Code	Error Message / Recommendation
38	Input file does not exist
39	This operation is not supported by service.
40	Metadata operation is skipped.
41	Error occurred during Metadata registration.
42	Error occurred during Metadata de-registration.

Special Error Cases for OMSPatcher OMS Automation

This section provides issue resolution information for special cases when using OMSPatcher. This information will allow the administrator to handle these issues easily with less need for support team intervention.

Windows patching failure due to lock of files by Oracle WebLogic Administration Server

In Windows operating systems, it has been noticed that some of the Enterprise Manager related files (used for patching) are locked by running of Oracle WebLogic Administration Server. As OMSPatcher required Oracle WebLogic Administration Server to be RUNNING for the configuration detection, we need to perform the following steps to make sure that this conflict with respect to environment and patching is removed.

1. Go to ORACLE_HOME
2. Run OMSPatcher in non-analyze mode. For further instructions, refer to the patch README and Administrator guide.

Once the OMSPatcher is run in non-analyze mode, it will check if active files are locked by Oracle WebLogic administration server and will provide a prompt as shown below (in silent mode it will be auto-yes):

```
Running prerequisite checks to verify if any files or services are locked by admin
server process...
Please monitor OPatch log file: c:\MW\oms\cfgtoollogs\opatch\1111112_Jun_
26_2024_08_16_19\ApplyPrereq2024-06-26_08-16-57AM_8.log
```

The details are:

```
Following files are active :
c:\MW\oms\sysman\jlib\emCoreConsole.jar
```

```
Due to active files to be patched, OMSPatcher will stop all OMS processes so tha
t lock on active files may be released...
Do you want to proceed? [y|n]
y
User Responded with: Y
OMSPatcher has stopped all OMS processes successfully.
```

If there is a failure while stopping OMS processes, OMSPatcher will accordingly error out. Refer to the OMSPatcher log file for details.

3. OMSPatcher will stop the stack and then ask for a confirmation from the administrator on whether to proceed with prerequisite checks of patch binaries (in silent mode it will be auto-yes):

OMSPatcher has stopped all OMS processes successfully. Please make sure the above listed active files are unlocked by all windows processes.
Do you want to proceed? [y|n] y

User Responded with: Y

Note

Administrators are requested to use some open source utilities like process explorer and search for file strings given as output in (2) to check if any files are still active. If so, kill the process tree of those files so that OPatch will run the checks, patch, and deploy the automation elements.

4. OMSPatcher will not attempt to re-start the stack. The administrator must restart the stack as needed.

A complete sample trace of this case is shown below:

```
C:\MW\oms\OPatch_June26>omspatcher apply ..\patches\cmdRcu\1111112
OMSPatcher Automation Tool
Copyright (c) 2024, Oracle Corporation. All rights reserved.

OMSPatcher version : 13.8.0.0.0
OUI version        : 13.8.0.0.0
Running from       : c:\MW\oms
Log file location  :
c:\MW\oms\cfgtoollogs\omspatcher\omspatcher2024-06-26_08-16-19AM_1.log

OMSPatcher log file:
c:\MW\oms\cfgtoollogs\omspatcher\1111112\opatch_oms_2024-06-26_08-16-23AM_deploy.log

Please enter the WebLogic Admin Server URL for primary OMS:> t3s://
example.o
racle.com:7101
Please enter the WebLogic Admin Server username for primary OMS:> weblogic
Please enter the WebLogic Admin Server password for primary OMS:>

Configuration Validation: Success

Running prerequisite checks to verify if any files or services are locked
by admin server process...
Please monitor OPatch log file:
c:\MW\oms\cfgtoollogs\omspatcher\1111112_Jun_26_2024_08_16_19\ApplyPrereq20
24-06-26_08-16-57AM_8.log

The details are:

Following files are active:
c:\MW\oms\sysman\jlib\emCoreConsole.jar

Due to active files to be patched, omspatcher will stop all OMS processes
so that lock on active files may be released...
Do you want to proceed? [y|n]
```

```
y
User Responded with: Y
omspatcher has stopped all OMS processes successfully.

omspatcher has stopped all OMS processes successfully. Please make sure
the above listed active files are unlocked by all windows processes.
Do you want to proceed? [y|n]
y
User Responded with: Y

Running apply prerequisite checks for patch(es) "1111112" and Oracle Home
"c:\MW
_130518\oms"...
Please monitor omspatcher log file:
c:\MW\oms\cfgtoollogs\omspatcher\1111112_Jun_26_2024_09_01_33\ApplyPrereq20
24-06-26_09-03-41AM_10.log
Patches "1111112" are successfully analyzed for Oracle Home "c:\MW\oms"

To continue, OMSPatcher will do the following:
[Patch and deploy patch(es) binaries] : Apply patch(es) [ 1111112 ] to
Oracle
Home "c:\MW\oms";
Apply RCU artifact with patch "c:\MW\oms\omspatcher_storage
\1111112_Feb_21_2024_06_30_38\original_patch"

Do you want to proceed? [y|n]
y
User Responded with: Y

Applying patch "1111112" to Oracle Home "c:\MW\oms"...
Please monitor OMSPatcher log file:
c:\MW\oms\cfgtoollogs\omspatcher\1111112_Jun_26_2024_09_01_33\apply2024-06-
26_09-04-17AM_12.log

Updating repository with RCU reference file
"c:\MW\oms\omspatcher_storage\1111112_Feb_21_2024_06_30_38\original_patch"

Copying all logs to:
c:\MW\oms\cfgtoollogs\omspatcher\2024-06-26_09-01-32AM_SystemPatch_1111112_
1

Patching summary:
Following patch(es) are successfully applied (Oracle home:patch list):
c:\MW\oms:1111112

Log file location:
c:\MW\oms\cfgtoollogs\omspatcher\1111112\omspatcher_oms_2023-06-26_09-01-36
AM_deploy.log

OMSPatcher succeeded.
```

OMSPatcher Session Resume

OMSPatcher supports resume upon failure capability for both single-OMS and multi-OMS configurations.

This section covers the following topics:

- [Resume capability in Single-OMS Configuration](#)
- [Resume Capability in Multi-OMS Configuration](#)

Resume capability in Single-OMS Configuration

On a single OMS System, OMSPatcher executes end-to-end automation of patching steps. Once a failure has occurred, OMSPatcher can resume from the failed step. The OMS administrator must refer to the master log file created by OMSPatcher to ascertain and resolve the root cause of the failure, and then run the `omspatcher resume` command to complete the patching. OMSPatcher resume runs the steps from the point of failure.

Example

1. OMSPatcher, while applying an auto system patch, it fails while stopping the OMS.

Example:

```
$omspatcher apply /scratch/patches_april/24_1_latest/1111112
OMSPatcher Automation Tool
Copyright (c) 2024, Oracle Corporation. All rights reserved.

OMSPatcher version : 13.9.24.2.0
OUI version       : 13.9.4.0.0
Running from      : /scratch/sm/work/omshome3308/oms_home
Log file location : /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/opath2025-04-11_15-28-54PM_1.log

OMSPatcher log file: /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/1111112/omspatcher_2025-04-11_15-29-13PM_apply.log

Please enter OMS weblogic admin server URL(t3s://
shortterm-16095.subnetlrg2phxsu.emdevinfra.phx1.oraclecn.com:7102):>
Please enter OMS weblogic admin server username(weblogic):>
Please enter OMS weblogic admin server password:>

Enter SYS or Non-SYS (Admin User) username: sys
Enter 'sys' password :
Checking if current repository database is a supported version
Current repository database version is supported

Prereq "checkComponents" for patch 1111140 passed.

Prereq "checkComponents" for patch 1111143 passed.

Prereq "checkComponents" for patch 1111142 passed.

Configuration Validation: Success

Running apply prerequisite checks for sub-patch(es) "1111140,1111143" and
```

```

Oracle Home "/scratch/sm/work/omshome3308/oms_home"...
Sub-patch(es) "1111140,1111143" are successfully analyzed for Oracle Home
"/scratch/sm/work/omshome3308/oms_home"

Running apply prerequisite checks for sub-patch(es) "1111142" and Oracle
Home "/scratch/sm/work/omshome3308/ext_oms_home"...
Sub-patch(es) "1111142" are successfully analyzed for Oracle Home "/"
scratch/sm/work/omshome3308/ext_oms_home"

To continue, OMSPatcher will do the following:
[Patch and deploy artifacts]   : Apply sub-patch(es) [ 1111140 1111143
1111142 ]
                                Apply sub-patch(es) [ 1111140 1111143
1111142 ]
                                Apply RCU artifact with patch "/"
scratch/sm/work/omshome3308/ext_oms_home/.omspatcher_storage/
1111142_Sep_12_2024_10_04_19/original_patch";
                                Apply RCU artifact with patch "/"
scratch/sm/work/omshome3308/oms_home/.omspatcher_storage/
1111143_Oct_9_2024_09_22_52/original_patch";
                                Register MRS artifact "swlib";
                                Register MRS artifact "eventsaux";
                                Register MRS artifact
"eventSpecificCustmzn";
                                Register MRS artifact "compression";
                                Register MRS artifact "oobrules";
                                Register MRS artifact "targetType";
                                Register MRS artifact "storeTargetType";
                                Register MRS artifact "jobTypes";
                                Register MRS artifact
"default_collection";
                                Register MRS artifact "omsPropertyDef";
                                Register MRS artifact "runbooks";
                                Register MRS artifact "TargetPrivilege"

Do you want to proceed? [y|n]
y
User Responded with: Y
Stopping all the services on primary OMS.....
Please monitor log file: /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/2025-04-11_15-36-55PM_SystemPatch_1111112_9/
stop_oms_all_2025-04-11_15-36-55PM.log

Complete Summary
=====

All log file names referenced below can be accessed from the directory "/"
scratch/sm/work/omshome3308/oms_home/cfgtoollogs/omspatcher/
2025-04-11_15-36-55PM_SystemPatch_1111112_9"

Patching summary:
-----

The following sub-patch(es) are applicable:

```

Featureset	Sub-
------------	------

```

patches                                Log file
-----                                -
-----                                -
oracle.sysman.top.oms    1111140,1111143
1111140,1111143_opatch2025-04-11_15-30-27PM_2.log
oracle.sysman.top.zdt    1111142
1111142_opatch2025-04-11_15-31-40PM_2.log

```

OMSPatcher failed to execute some of the patching steps. Please check the Patching summary, individual logs and try to resolve the issue. Once the issue is resolved, Please execute below command to complete patching session:

```
omspatcher resume
```

```

-----
-----
OMSPatcher wont allow any other patching operations unless the script is
executed successfully
-----
-----

```

Log file location: /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/1111112/omspatcher_2025-04-11_15-29-13PM_apply.log

OMSPatcher failed with error code 240

2. OMS Administrator cannot start a new patching session when there are remnants of an incomplete patching session. OMSPatcher clearly errors out with the detailed information regarding the failure and what action need to be taken to fix this issue.

Example:

```

omspatcher apply /scratch/patches_april/24_1_latest/1111112
OMSPatcher Automation Tool
Copyright (c) 2024, Oracle Corporation. All rights reserved.

```

```

OMSPatcher version : 13.9.24.2.0
OUI version        : 13.9.4.0.0
Running from       : /scratch/sm/work/omshome3308/oms_home
Log file location  : /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/opatch2025-04-11_17-05-39PM_1.log

```

OMSPatcher finds that previous patching session is not yet completed. Please refer log file for the previous session and execute the below command to complete the previous session. OMSPatcher can proceed to execute new operations only if previous session is completed successfully.

```
omspatcher resume
```

Log file location: /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/opatch2025-04-11_17-05-39PM_1.log

OMSPatcher failed with error code 255

3. Now OMS Administrator can run the `omspatcher resume` command on the single OMS to finish the failed patching session.

Example:

```

OMSPatcher/omspatcher resume
OMSPatcher Automation Tool
Copyright (c) 2024, Oracle Corporation. All rights reserved.

OMSPatcher version : 13.9.24.2.0
OUI version       : 13.9.4.0.0
Running from      : /scratch/sm/work/omshome3308/oms_home
Log file location : /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/opatch2025-04-11_17-07-40PM_1.log

OMSPatcher log file: /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/SystemPatch/omspatcher_2025-04-11_17-07-13PM_resume.log

[Info:Previous action was performed by user:'sys']
Enter 'sys' password :
Enter SYSMAN Password :
command /scratch/sm/work/omshome3308/oms_home/bin/emctl stop oms -all -
force
/scratch/sm/work/omshome3308/oms_home/bin/emctl stop oms -all -force is
Successfully run
.....

command /scratch/sm/work/omshome3308/oms_home/OMSPatcher/omspatcher
executeCommand -cmdType POST_APPLY_SQL -oh /scratch/sm/work/omshome3308/
oms_home -dbUser sys
/scratch/sm/work/omshome3308/oms_home/OMSPatcher/omspatcher executeCommand
-cmdType POST_APPLY_SQL -oh /scratch/sm/work/omshome3308/oms_home -dbUser
sys is Successfully run

command /scratch/sm/work/omshome3308/oms_home/bin/emctl start oms
/scratch/sm/work/omshome3308/oms_home/bin/emctl start oms is Successfully
run

OMSPatcher succeeded.

```

Resume Capability in Multi-OMS Configuration

On a multi-OMS System, OMSPatcher executes end-to-end automation of patching steps. Once a failure has occurred, OMSPatcher can resume from the failed step. The OMS administrator must refer to the master log file created by OMSPatcher to ascertain and resolve the root cause of the failure, and then run the `omspatcher resume` command to complete the patching. OMSPatcher resume runs the steps from the point of failure.

For Multi-OMS configuration, OMSPatcher resume runs on the primary OMS and automatically completes the patching on add OMSes by submitting the job.

Example

1. OMSPatcher, while applying an auto system patch, it fails while stopping the OMS.

Example:

```

$omspatcher apply /scratch/patches_april/24_1_latest/1111112
OMSPatcher Automation Tool

```

Copyright (c) 2024, Oracle Corporation. All rights reserved.

```
OMSPatcher version : 13.9.24.2.0
OUI version       : 13.9.4.0.0
Running from      : /scratch/sm/work/omshome3308/oms_home
Log file location : /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/patch2025-04-11_15-28-54PM_1.log
```

```
OMSPatcher log file: /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/1111112/omspatcher_2025-04-11_15-29-13PM_apply.log
```

```
Please enter OMS weblogic admin server URL(t3s://
shortterm-16095.subnet1rg2phxsu.emdevinfra.phx1.oraclecn.com:7102):>
Please enter OMS weblogic admin server username(weblogic):>
Please enter OMS weblogic admin server password:>
```

```
Enter SYS or Non-SYS (Admin User) username: sys
Enter 'sys' password :
Checking if current repository database is a supported version
Current repository database version is supported
```

```
Prereq "checkComponents" for patch 1111140 passed.
```

```
Prereq "checkComponents" for patch 1111143 passed.
```

```
Prereq "checkComponents" for patch 1111142 passed.
```

```
Configuration Validation: Success
```

```
Running apply prerequisite checks for sub-patch(es) "1111140,1111143" and
Oracle Home "/scratch/sm/work/omshome3308/oms_home"...
Sub-patch(es) "1111140,1111143" are successfully analyzed for Oracle Home
"/scratch/sm/work/omshome3308/oms_home"
```

```
Running apply prerequisite checks for sub-patch(es) "1111142" and Oracle
Home "/scratch/sm/work/omshome3308/ext_oms_home"...
Sub-patch(es) "1111142" are successfully analyzed for Oracle Home "/"
scratch/sm/work/omshome3308/ext_oms_home"
```

```
To continue, OMSPatcher will do the following:
```

```
[Patch and deploy artifacts] : Apply sub-patch(es) [ 1111140 1111143
1111142 ]
```

```
Apply sub-patch(es) [ 1111140 1111143
```

```
1111142 ]
```

```
Apply RCU artifact with patch "/"
scratch/sm/work/omshome3308/ext_oms_home/.omspatcher_storage/
1111142_Sep_12_2024_10_04_19/original_patch";
```

```
Apply RCU artifact with patch "/"
scratch/sm/work/omshome3308/oms_home/.omspatcher_storage/
1111143_Oct_9_2024_09_22_52/original_patch";
```

```
Register MRS artifact "swlib";
Register MRS artifact "eventsaux";
Register MRS artifact
```

```
"eventSpecificCustmzn";
```

```
Register MRS artifact "compression";
Register MRS artifact "oobrules";
```

```

Register MRS artifact "targetType";
Register MRS artifact "storeTargetType";
Register MRS artifact "jobTypes";
Register MRS artifact
"default_collection";

Register MRS artifact "omsPropertyDef";
Register MRS artifact "runbooks";
Register MRS artifact "TargetPrivilege"

Do you want to proceed? [y|n]
y
User Responded with: Y
Stopping all the services on primary OMS.....
Please monitor log file: /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/2025-04-11_15-36-55PM_SystemPatch_1111112_9/
stop_oms_all_2025-04-11_15-36-55PM.log

```

Complete Summary
=====

All log file names referenced below can be accessed from the directory "/
scratch/sm/work/omshome3308/oms_home/cfgtoollogs/omspatcher/
2025-04-11_15-36-55PM_SystemPatch_1111112_9"

Patching summary:

The following sub-patch(es) are applicable:

patches	Featureset	Sub-	Log file
-----	-----		-----
oracle.sysman.top.oms	1111140,1111143		
1111140,1111143_opatch			2025-04-11_15-30-27PM_2.log
oracle.sysman.top.zdt	1111142		
1111142_opatch			2025-04-11_15-31-40PM_2.log

OMSPatcher failed to execute some of the patching steps. Please check the
Patching summary, individual logs and try to resolve the issue. Once the
issue is resolved, Please execute below command to complete patching
session:

```
omspatcher resume
```

```

-----
OMSPatcher wont allow any other patching operations unless the script is
executed successfully
-----

```

Log file location: /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/1111112/omspatcher_2025-04-11_15-29-13PM_apply.log

OMSPatcher failed with error code 240

2. OMS Administrator cannot start a new patching session when there are remnants of an incomplete patching session. OMSPatcher clearly errors out with the detailed information regarding the failure and what action need to be taken to fix this issue.

Example:

```
omspatcher apply /scratch/patches_april/24_1_latest/1111112
OMSPatcher Automation Tool
Copyright (c) 2024, Oracle Corporation. All rights reserved.
```

```
OMSPatcher version : 13.9.24.2.0
OUI version        : 13.9.4.0.0
Running from       : /scratch/sm/work/omshome3308/oms_home
Log file location  : /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/opatch2025-04-11_17-05-39PM_1.log
```

```
OMSPatcher finds that previous patching session is not yet completed.
Please refer log file for the previous session and execute the below
command to complete the previous session. OMSPatcher can proceed to
execute new operations only if previous session is completed successfully.
omspatcher resume
```

```
Log file location: /scratch/sm/work/omshome3308/oms_home/cfgtoollogs/
omspatcher/opatch2025-04-11_17-05-39PM_1.log
```

```
OMSPatcher failed with error code 255
```

3. Now OMS Administrator can run the `omspatcher resume` command on the primary OMS to finish the failed patching session.

Example:

```
OMSPatcher/omspatcher resume
```

Patching Oracle Management Agents

This chapter describes how to patch Oracle Management Agents (Management Agents) in Enterprise Manager.

This chapter consists of the following sections:

- [Overview](#)
- [Automated Management Agent Patching Using Patch Plans \(Recommended\)](#)
- [Manual Management Agent Patching](#)

Overview

Management Agent patches are released to fix one or more errors related to Management Agent targets. You can patch Management Agents that are deployed on OMS hosts, as well as remote hosts.

Agent System Patches

Agent patches are consolidated into one single system patch model. The consolidated agent system patch contains:

- Agent platform patch
- Agent plugin patches
 - Monitoring patch
 - Discovery patch

Separate Management Agent patches for core components of the Management Agent and every agent plugin (monitoring and discovery) are no longer necessary. Instead, comprehensive *system patches* are produced for each Enterprise Manager release update which contains all sub-patches for agent-side platform and monitoring and discovery patches for the agent plugins.

Identifying Patch Release Update Versions

The patch release update version is now embedded as part of each agent system patch in order to help you identify which release update version has been deployed on Monitoring Agents. To view which patch release update version has been deployed on a specific agent, do the following:

1. From the **Setup** menu, select **Manage Enterprise Manager** and then **Agents**. A list of agents displays.
2. Click on the desired agent to access that agent's home page.
3. From the **Agent** drop-down menu, select **Properties**.
4. Scroll down to the `_agentRUVersion` property. The value shown identifies the release update patch version that has been applied to that agent.
For example, if `_agentRUVersion` shows 13.5.0.1, then it means Release Update 1 has been applied on that agent. The last digit indicates the Agent Release Update version.

Patch Installation Methods

You can apply Management Agent patches using the automated approach (that is, using patch plans) or the manual approach. Oracle recommends using the automated approach to carry out your patching operations. This approach not only saves time and effort while mass-deploying patches, but also reduces human intervention, thereby minimizing the errors involved while patching. For more information about this approach, see [Automated Management Agent Patching Using Patch Plans \(Recommended\)](#).

If you are unable to patch your Management Agent using patch plans, you can use the manual patching approach. However, this approach is not recommended. For more information about this approach, see [Manual Management Agent Patching](#).

① Note

System patches are fully compatible with Enterprise Manager Patch Plan functionality, so there is no need to change your patching methodology if you're using Patch Plan.

Automated Management Agent Patching Using Patch Plans (Recommended)

Automated patching is a quick, easy, and reliable patching mechanism that is facilitated using patch plans in Enterprise Manager. Patch plans can be created, accessed, and deployed using the Enterprise Manager console, or EM CLI. For large scale deployments, you can use EM CLI to create, access, and deploy patch plans. This section only describes how to patch your Management Agent targets using the Enterprise Manager console. For information about

patching targets using EM CLI, see *Patching Using EM CLI* in the *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

Automated patching can be performed while Enterprise Manager is running in the Online mode, as well as the Offline mode. When Enterprise Manager is running in the Online mode, you can connect to *My Oracle Support* to download the patches that you want to apply. However, if Enterprise Manager is running in the Offline mode, you must ensure that the patches that you want to apply are already available in Oracle Software Library (Software Library).

This section consists of the following:

- [Advantages of Automated Management Agent Patching](#)
- [Accessing the Patches and Updates Page](#)
- [Viewing Patch Recommendations](#)
- [Searching for Patches](#)
- [Applying Management Agent Patches](#)
- [Verifying the Applied Management Agent Patches](#)
- [Management Agent Patching Errors](#)

Advantages of Automated Management Agent Patching

The advantages of patching your Management Agent targets using the automated approach (as compared to the manual approach) are:

- Patching operations are more organized, done through a single window, and are always initiated only from the OMS.
- This approach allows you to schedule periodic patching jobs that connect to *My Oracle Support*, check for the latest patches, and automatically download them. This saves the effort involved in searching for the latest patches and patch sets, and downloading them whenever they are available.

Note

Only a single system patch can be added to a patch plan. For more information about Agent System Patches, see [Overview: Agent System Patches](#).

Accessing the Patches and Updates Page

To access the Patches and Updates page in Enterprise Manager, from the **Enterprise** menu, select **My Oracle Support**, then select **Patches & Updates**.

Viewing Patch Recommendations

Patch recommendations are proactive notifications of potential system problems and recommendations that help you improve system performance and avert outages. Patch recommendations minimize the effort required to search for the critical patches that must be applied on your targets.

The Patch Recommendations section is available on the Patches and Updates page. The patches in this section are classified as security patches, and other recommended patches.

For more information about patch recommendations, see *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

Searching for Patches

This section consists of the following:

- [Searching for Patches On My Oracle Support](#)
- [Searching for Patches in Software Library](#)

Searching for 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 enables you to perform searches quickly and efficiently.

To search for a patch on My Oracle Support, follow these steps:

1. From the **Enterprise** menu, select **My Oracle Support**, then select **Patches & Updates**.
2. To perform a simple search, in the Patch Search region, select **Number/Name or Bug Number (Simple)**, then specify the patch name, patch number, or the bug number. Click **Search**.

To perform an advanced search, select **Product or Family (Advanced)**, then specify the product, release, and any other criteria you wish to use for the patch search.

Alternatively, you can use the **Saved** tab to search for previously saved searches. You can also use the **Recent** tab to access any recently performed searches.

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 or to Software Library.

Searching for Patches in Software Library

By default, when you search for a patch on the Patches & Updates page, Enterprise Manager connects to My Oracle Support using the Internet connectivity available on that host, and searches for the requested patch on 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 Software Library.

To switch over to offline mode, follow these steps:

1. From the **Setup** menu, select **Provisioning and Patching**, then select **Offline Patching**.
2. For **Connection**, 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 for a patch in Software Library, follow these steps:

1. From the **Enterprise** menu, select **My Oracle Support**, then select **Patches & Updates**.
2. To perform a simple search, in the Software Library Patch Search region, select **Number/ Name or Bug Number (Simple)**, then specify the patch name, patch number, or the bug number. Click **Search**.

To perform an advanced search, select **Product or Family (Advanced)**, then specify the product, release, and any other criteria you wish to use for the patch search.

Alternatively, you can use the **Saved** tab to search for previously saved searches. You can also use the **Recent** tab to access any recently performed searches.

Once the patch search is complete, the results appear in the **Patch Search Results** page.

Applying Management Agent Patches

To apply Management Agent patches using patch plans, follow these steps:

Note

- You can use patch plans to apply system patches. The process is described later in this section.
- For a large scale deployments, you can use EM CLI. For information about patching using EM CLI, see *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

1. In Enterprise Manager, from the **Enterprise** menu, select **My Oracle Support**, then select **Patches and Updates**.
2. On the Patches and Updates page, select the Management Agent patches that you want to apply from the Patch Recommendations section, or the Patch Search section.

For more information on the Patch Recommendation section, see [Viewing Patch Recommendations](#). For more information on how to search for patches, see [Searching for Patches](#).

3. From the context menu that appears, select one of the following options:
 - **Add to New:** Select this option if you want to create a new patch plan that has the selected patch.

Specify a plan name, the targets that you want to patch, then click **Create Plan**.

The patch and the associated targets are added to the patch plan.

- **Add to Existing Plan:** Select this option if you want to add the selected patch to an existing patch plan.

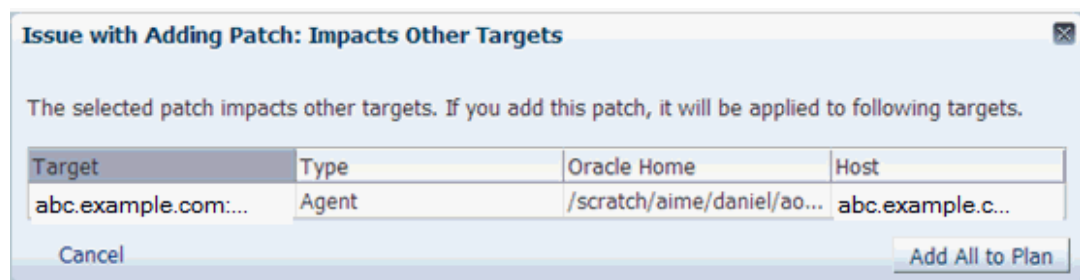
Select the existing patch plan that you want to add the required patch to, specify the patch targets, then click **Add Patch to Plan**.

Note

Ensure that the patches you select have the same platform as the targets that you want to patch. For example, Linux x86-64 patches can be applied only on Linux x86-64 targets. Any mismatch will result in a patching error.

4. If the selected patches are applied on homogeneous targets, then the patch plan is created successfully with a link to view the patch plan. Click the link to view the patch plan details.

If any of the Management Agent targets added to the patch plan are shared agents or cluster Management Agents, then you may see a warning message mentioning that there are issues with adding the patch to the patch plan.



As a solution to this problem, click **Add All To Plan** to add all the affected targets to the patch plan.

However, if the platform of the selected patch does not match the platform of the selected target, you may see one of the following errors or warnings:

- A null platform error occurs when the selected target appears with a null platform. The patch plan validation fails as platform of the patch and the platform of the target do not match. This may occur when a target is down. In this case, the patch plan is not created until the error is fixed.
- A platform mismatch warning appears when the platform of the patch and the platform of a target do not match. This target is ignored, and the patch plan is created without this target. The other homogeneous targets are added to the plan.

Note

Oracle recommends that you fix the warnings before proceeding, as they may result in an error during patch plan validation. However, if you want to proceed regardless, you can select **Ignore Warnings and Add**.

5. Navigate to the Patches & Updates page. In the Plans region, click the name of the patch plan that you want to view.

The Create Plan wizard is displayed.

6. 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) Enter a short description for the patch plan.
 - c. (Optional) In the Allow Access For section, click **Add** to grant patch plan access permissions to administrators or roles for the current patch plan.

In the Add Privileges to Administrators window, select an administrator or a role, the access permission that you want to grant, then click **Add Privilege**.
 - d. Click **Next**.
7. On the Patches page, review the patches added to the patch plan.

To add new patches to the patch plan or add additional targets to a patch that has already been added to the patch plan, click **Add Patch**. In the Edit Search dialog box, enter the patch number, then click **Search**. Select the required patch, then click **Add to This Plan**. Select the targets that you want to add to the patch, then click **Add to This Plan**.

Click **Next**.
8. 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 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, navigate to the location (parent directory) where you want to stage the patch, create a subdirectory with the same name as the patch ZIP file, then extract the contents of the patch ZIP file in this subdirectory. In the Where to Stage section, enter the absolute path to the parent directory where you have manually staged the patches.

For example, if you downloaded patch 699099.zip, and 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 of the zip file. Enter /u01/app/oracle/em/stagepatch as the stage path.
 - b. In the Credential Information section, provide the required credentials for patching. You can choose to use preferred credentials, or override the preferred credentials with different credentials.

If the patches that you want to apply on the Management Agent targets require *root* user access to perform certain tasks, then you must provide the privileged Oracle home credentials for the Management Agent targets.

If the Management Agent targets that you want to patch are not secure, then you must set the preferred Management Agent host credentials for all the Management Agent targets that you want to patch. To set the preferred host credentials for Management Agent targets, from the **Setup** menu, select **Security**, then select **Preferred Credentials**. Select the **Agent** target type, then click **Manage Preferred Credentials**. Set the preferred host credentials for the required Management Agent targets.

For more information about setting preferred credentials, see *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

Note

The named credentials of type *SSH Key Credentials* cannot be set as the normal host preferred credentials or the privileged host preferred credentials for Oracle home targets.

Click **Validate Credentials** to verify the accuracy of the provided credentials.

- c. In the Notification section, specify whether or not you want to enable email notifications when the patch plan is scheduled, starts, requires action, is suspended, succeeds, and fails.

To enable email notifications, select **Receive notification emails when the patching process**, then select the required options. If a warning message, mentioning that the sender or the receiver email address is not set up, is displayed, perform the action mentioned in the warning.

- d. In the Rollback section, select **Rollback patches in the plan** to roll back the patches listed in the plan, rather than deploy them.

Note

For Enterprise Manager 13c Release 5 and later, the **Rollback patches in the plan** option is no longer supported.

- e. In the OPatch Upgrade section, select **OPatch Upgrade** to upgrade the OPatch component before the patching operation begins.

For the OPatch component to be upgraded, ensure that it is downloaded and unzipped to the same location where the patches that you want to apply are staged.

- f. In the *Conflict Check* section, specify whether you want to enable or disable ARU Conflict Check, a check that uses Oracle Automated Release Updates (ARU) to search for patch conflicts within the patch plan during the analysis stage. Also, specify the action that the patching procedure must take when a patch conflict is encountered during deployment.

For **Conflicts**, select **Stop at Conflicts** if you want the patching procedure to stop the deployment of the plan when a conflict is encountered, select **Force Apply** if you want the patching procedure to roll back the conflicting patches and apply the incoming patches when a conflict is encountered, or select **Skip conflicts** if you want the patching procedure to apply only the non-conflicting patches, and skip the application of the conflicting patches, when a conflict is encountered.

Note

For Enterprise Manager 13c Release 5, *Conflict Check* is no longer applicable with the advent of system patches.

- g. Click **Next**.
- 9. On the Validation page, click **Analyze** to validate the patch before deploying it. A validation job is submitted, which checks for patch conflicts, checks for the latest OPatch version, checks if the version and platform of the targets and the patch are the same, and so on. To track the progress of the validation job, click **Show Detailed Results**.

Alternatively, you can navigate directly to the Review and Deploy page to deploy the Management Agent patches without analyzing the plan. If you do so, a deploy job is submitted which analyzes the plan, and deploys it on successful analysis.

Note

If any problems are encountered during the analysis phase, then the split plan feature is enabled, in which the patch plan is split into two patch plans, one having the targets for which the analysis failed, and another having the targets for which the analysis was successful. The patch plan having the targets for which the analysis was successful is available for deployment, while the other patch plan must be reanalyzed and deployed separately.

Upon validation, if there are conflicts between two patches, then it is recommended that you request for replacement patches. In this case, click **Request Replacement Patches**. If there is a merge patch already available for the conflicting patches, you can choose to directly replace the conflicting patches with the merge patch. To do this, click **Replace Conflicting Patches**.

For information about the errors that may occur during the validation phase, see [Management Agent Patching Errors](#).

Click **Next**.

10. On the Review & Deploy page, review the details that you have provided for the patch plan, then click **Deploy**.

Once you click **Deploy**, a Deploy Confirmation dialog box appears, which enables you to schedule the Deploy operation. Select **Deploy**. If you want to begin the Deploy operation immediately, select **Immediately**. If you want to schedule the Deploy operation such that it begins at a later time, select **Later**, then specify the time. Click **Submit**.

After scheduling a deploy operation, the **Deploy** button on the Review and Deploy page is renamed to **Reschedule**. If you want to reschedule the Prepare or Deploy operation, click **Reschedule**, specify the time, then click **Submit**. If you want to discard the schedule and bring the patch plan back to its last valid state, click **Stop Schedule**. Note that the deploy operation schedule is discarded if you edit a patch plan deployment option or a patch target. In this case, you must validate the patch plan again.

A deploy job is submitted. To track the progress of the job, click **Show Detailed Results**.

Verifying the Applied Management Agent Patches

To verify the applied Management Agent patches, perform the following steps:

1. In Enterprise Manager, from the **Targets** menu, select **All Targets**.
2. On the All Targets page, for the **Search Target Name** field, enter the name of the Management Agent target that you just patched, then click the search icon. Click the name of the required target.
3. On the Management Agent target home page, under the Summary section and the Configuration sub-section, click **Oracle Home and Patch Details** to view all the jobs that have run on the Oracle home target of the Management Agent.
4. Under the Patch Advisories section, select the **Patches Applied** tab to verify all the patches that have been applied successfully on the Management Agent target.

Management Agent Patching Errors

The following are some of the errors that you may encounter while patching Management Agent targets:

- [Oracle Home Credentials Are Not Set](#)
- [Management Agent Target Is Down](#)
- [Patch Conflicts Are Detected](#)
- [User Is Not a Super User](#)
- [Patch Is Not Staged or Found](#)

Oracle Home Credentials Are Not Set

Error Description

This error occurs when the preferred Management Agent host credentials (for patching Management Agents that are not secure), or the privileged Oracle home credentials (for patches that require *root* user access) are not set.

Workaround

If the Management Agent targets that you want to patch are not secure, set the preferred Management Agent host credentials for all these targets. To set the preferred host credentials for a Management Agent target, from the **Setup** menu, select **Security**, then select **Preferred Credentials**. Select the **Agent** target type, then click **Manage Preferred Credentials**. Set the preferred host credentials for the Management Agent target. Analyze and deploy the patch plan.

If the patches that you want to apply (on the Management Agent targets) require *root* user access, set the privileged Oracle home credentials for the Management Agent targets. Analyze and deploy the patch plan.

Management Agent Target Is Down

Error Description

This error occurs when the Management Agent target added for patching is not up and running.

Workaround

Start the Management Agent target, then analyze and deploy the patch plan.

Patch Conflicts Are Detected

Error Description

This error occurs when there is a conflict between two added patches.

Workaround

Do one of the following:

- Contact Support to obtain a merged patch.
- Choose the advanced OPatch options to force apply the patch. However, choosing this option and applying the patch will result in the loss of earlier patch changes.

User Is Not a Super User

Error Description

This error occurs when the user that runs the patch plan does not have *root* access.

Workaround

Follow these steps:

1. Create a new credential that has *root* access.
2. Ensure that privilege delegation settings have been configured on the target Management Agent host.
3. Analyze and deploy the patch plan.

Patch Is Not Staged or Found

Error Description

This error occurs when the patch is not present in the stage location.

Workaround

Ensure that the patch is available in the stage location. Analyze and deploy the patch plan.

Manual Management Agent Patching

Manual patching is a patching mechanism that requires you to follow step-by-step instructions to patch a Management Agent manually. This mechanism of patching requires you to ensure certain prerequisites, manually validate the patch for applicability and conflicts, and can be used to patch only a single Management Agent at a time.

Note

Oracle recommends that you use the automated patching mechanism as it not only saves time and effort in mass-deploying patches, but also reduces human intervention, thereby minimizing the errors involved during the patching process.

To patch a Management Agent target manually, perform the following steps:

1. Log into [My Oracle Support \(https://support.oracle.com\)](https://support.oracle.com).

Note

Ensure that you check the Patch Recommendation section to view the patches that are recommended for your environment.

2. On the My Oracle Support home page, click **Patches and Updates**.
3. Enter the required patch number in the Patch Search section, then click **Search**.
4. Select the patch, and from the context menu that appears, select **Download**.

5. Extract the patch zip file and follow the instructions available in `Readme.html` or `Readme.txt` to install the patch.

 **Note**

In Enterprise Manager 13c Release 4 and earlier, separate Management Agent patches exist for core components of Management Agents and Management Agent plug-ins. Ensure that you navigate to the correct directory location under `<agent_base_directory>` while manually patching a Management Agent core component or a Management Agent plug-in. For more information on Agent patching, see *Applying Patches to Oracle Management Agents While Deploying or Upgrading Them*.

This does not apply to Enterprise Manager 13c Release 5 and later: Agent System Patches consolidate all required patches.

6

Personalizing Enterprise Manager

You can personalize the page layout and data displayed in certain Enterprise Manager pages, including target home pages such as Group, System, Oracle HTTP Server, and so on. The changes you make are persisted for the currently logged in user, enabling you to create customized consoles for monitoring various target types.

Note that not all pages in Enterprise Manager can be personalized. The page edit mode will only be enabled for those pages or page regions that can be modified.

This chapter contains the following sections:

- [Personalizing a Enterprise Manager Page](#)
- [Customizing a Region](#)
- [Setting Your Homepage](#)
- [Setting Pop-Up Message Preferences](#)

Personalizing a Enterprise Manager Page

Pages in Enterprise Manager are laid out in a columnar format. Each column contains one or more *regions*, each of which contains data rendered as a bar chart, graph or other visual component.

You can modify the layout of columns within a page, as well as select the regions to display within each column, enabling you to personalize how the data on a page is arranged and displayed.

To personalize a page:

1. Navigate to the page you want to personalize.
2. Select **Personalize Page** from the menu item that displays the username of the currently logged-in user. In the following graphic, the menu item displays the SYSMAN user name.

Note that the menu item will only be enabled if the page you are currently on can be personalized.
3. You are now in page edit mode. Click the **Change Layout** button. A graphical menu of column layout options opens.
4. Select the column layout you want to use.
5. Next, add a region to each column. Click the **Add Content** button for a specific column. The Resource Catalog, which contains available components used to display data, opens.
6. Select a region, then click **Add** to add it to the column. Note that you can “stack” regions on top of one another.
7. Once a region has been added to a column, you can:
 - Customize the region. See [Customizing a Region](#) for details.
 - Click the **View Actions** menu in the upper right corner of the region to move the region up or down within the column.

- Drag the region from one column to another.
8. Click **Close** to save your changes.

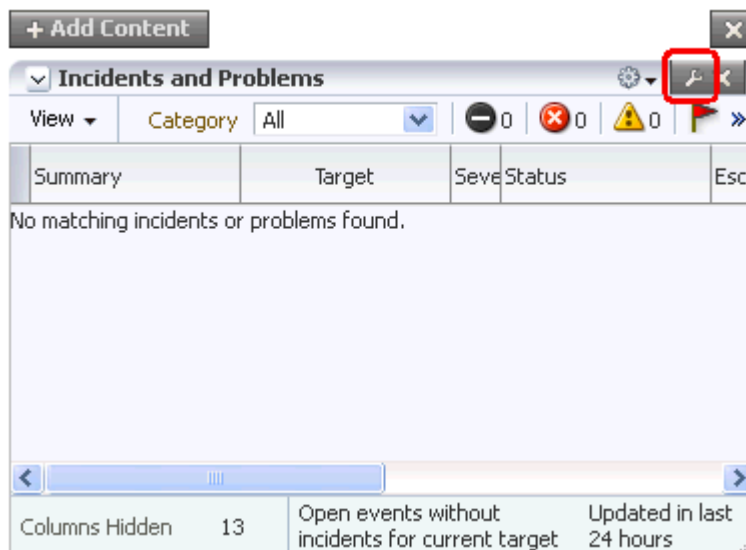
Customizing a Region

A *region* contains business data rendered as a bar chart, graph or other visual component. You can select the component to display within a specific region.

To customize a region within a page column:

1. Navigate to the page containing the region you want to customize and enable the page editing mode as described in [Personalizing a Enterprise Manager Page](#).
2. Click the "ratchet" icon next to the "X" icon within a region, as shown in [Figure 6-1](#). Note that the icon will only be enabled if the region can be customized.

Figure 6-1 Customize Region Icon



For most resources, you will specify the target host from which to collect data.

Other configurable parameters and customization options vary between regions. When you click the icon, a dialog opens to enable you to specify parameters, such as target type, target name and metric name.

3. If at a later time you want to remove the region from the page, click the "X" icon in the region.
4. Click **Close** to save your changes.

Setting Your Homepage

Enterprise Manager allows you to choose the page that will serve as your homepage - the first page you see after logging in to Enterprise Manager. You can either:

- Choose your own page, such as a target homepage that you view frequently or have customized to suit your specific needs

- Select from a pre-designed homepage templates created for specific types of Enterprise Manager users

Choosing Your Own Homepage

1. Navigate to the page you want to set as your homepage.
2. Select **Set Current Page As My Home** from the menu item that displays the username of the currently logged-in user.

Your homepage is saved as a "favorite" page. To de-select your current homepage:

1. From the **Favorites** menu, select **Manage Favorites**.
2. Select your homepage from the list, then click the **Remove Selected** button.
3. Click **OK** when finished.

Setting Pop-Up Message Preferences

The Pop-Up Message Preferences page allows you to select the messages from different sub-components, that you would like to display in real-time to the user on any page in the Enterprise Manager console.

Notification messages such as target status change and command-line broadcast messages from Super Administrators can be displayed by making appropriate setting changes on this page. By default, the pop-up messages are set to **Show** status.

If you want to retain the 'Show' status for these pop-up messages, you can set the **Show System Broadcast sent by the super administrator using EMCLI**.

This option enables you to see all the messages sent by the super administrator. By default, the messages appear on all the screens in the Enterprise Manager console. If you deselect this option, the messages will not be displayed on any screen.

For example, if you run the following command, a broadcast with the custom message appears on every screen of the Enterprise Manager console.

```
emcli send_system_broadcast -messageType="INFO" -toOption="ALL" -message="EM will be taken down in an hour for an emergency patch"
```

The messages are usually transient and last for a stipulated amount of time on a particular page. However, for command line messages, there is an added flexibility in terms of allowing the message to stay on the page until the user chooses to close it.

The following message types are supported:

- Confirmation
- Information
- Warning
- Error
- Fatal

By default, the duration for message display is **15 seconds**. You can change this value, if required. To change, specify the duration you want in the **Number of seconds to show the System Broadcast** field and click **Save**.

Administering Enterprise Manager Using EMCTL Commands

Enterprise Manager Control (EMCTL) is a command line utility installed with EM to administer or control the core components of Enterprise Manager, particularly Oracle Management Service (OMS) and Oracle Management Agent (Management Agent). The utility is available by default with every Enterprise Manager installation.

This chapter explains the following:

- [Executing EMCTL Commands](#)
- [Guidelines for Starting Multiple Enterprise Manager Components on a Single Host](#)
- [Starting and Stopping Oracle Enterprise Manager](#)
- [Services That Are Started with Oracle Management Service Startup](#)
- [Starting and Stopping the Oracle Management Service and Management Agent on Windows](#)
- [Reevaluating Metric Collections Using EMCTL Commands](#)
- EMCTL Commands:
 - [EMCTL Commands for OMS](#)
 - [EMCTL Commands for Management Agent](#)
 - [EMCTL Security Commands](#)
 - [EMCTL HAConfig Commands](#)
 - [EMCTL Resync Commands](#)
 - [EMCTL Connector Command](#)
 - [EMCTL Patch Repository Commands](#)
 - [EMCTL Commands for Windows NT](#)
 - [EMCTL Partool Commands](#)
 - [EMCTL Plug-in Commands](#)
 - [EMCTL Command to Sync with OPSS Policy Store](#)
- Troubleshooting:
 - [Troubleshooting Oracle Management Service Startup Errors](#)
 - [Troubleshooting Management Agent Startup Errors](#)
 - [Using emctl.log File to Troubleshoot](#)

Executing EMCTL Commands

In UNIX systems, to run EMCTL commands for Oracle Management Service (OMS), navigate to the <OMS_HOME>/bin directory and run the desired command. To run EMCTL commands for

Management Agent, navigate to the `<AGENT_HOME>/bin` directory and run the desired command.

Similarly, for Windows systems, to run EMCTL commands for OMS, navigate to the `<OMS_HOME>\bin` directory and to `<AGENT_HOME>\bin` directory for Management Agent commands.

Guidelines for Starting Multiple Enterprise Manager Components on a Single Host

Oracle Enterprise Manager components are used to manage a variety of Oracle software products. In most cases, in a production environment, you will want to distribute your database and WebLogic Server instances among multiple hosts to improve performance and availability of your software resources. However, in cases where you must install multiple WebLogic Servers or databases on the same host, consider the following guidelines.

When you start Fusion Middleware Control, the Management Agent, or Database Control, Enterprise Manager immediately begins gathering important monitoring data about the host and its managed targets. Keep this in mind when you develop a process for starting the components on the host.

Specifically, consider staggering the startup process so that each Enterprise Manager process has a chance to start before the next process begins its startup procedure. Using a staggered startup procedure ensures that the processes are not in contention for resources during the CPU-intensive startup phase for each component. However, in the case of a system restart, `/etc/init.d/gcstartup` script which is registered during the EM deployment ensures that the OMS and the Management Agent are started automatically in a staggered manner.

Starting and Stopping Oracle Enterprise Manager

The following sections describe how to stop and start all the Enterprise Manager components that are installed by the Oracle Enterprise Manager console installation procedure.

You can use these procedure to start all the framework components after a system reboot or to shutdown all the components before bringing the system down for system maintenance.

The following procedures are covered under this section:

- [Starting Enterprise Manager and All Its Components](#)
- [Stopping Enterprise Manager and All Its Components](#)

Starting Enterprise Manager and All Its Components

The following procedure summarizes the steps required to start all the components of Enterprise Manager. For example, use this procedure if you have restarted the host computer and all the components of Enterprise Manager have been installed on that host.

To start all Enterprise Manager components on a host, use the following procedure:

1. If your Oracle Management Repository resides on the host, change directory to the Oracle Home for the database where you installed the Management Repository and start the database and the Net Listener for the database:
 - a. Set the `ORACLE_HOME` environment variable to the Management Repository database home directory.

- b. Set the ORACLE_SID environment variable to the Management Repository database SID (default is asdb).
 - c. Start the Net Listener:

```
$PROMPT> $ORACLE_HOME/bin/lsnrctl start
```
 - d. Start the Management Repository database instance:

```
ORACLE_HOME/bin/sqlplus /nolog
SQL> connect SYS as SYSDBA
SQL> startup
SQL> quit
```
2. Start the Oracle Management Service:

```
$PROMPT> OMS_HOME/bin/emctl start oms
```
3. Change directory to the home directory for the Oracle Management Agent and start the Management Agent:

```
$PROMPT> AGENT_HOME/bin/emctl start agent
```

Note

Be sure to run the `emctl start agent` command in the Oracle Management Agent home directory and not in the Management Service home directory.

Stopping Enterprise Manager and All Its Components

The following procedure summarizes the steps required to stop all the components of Enterprise Manager. For example, use this procedure if you have installed all the components of Enterprise Manager on the same host you want to shut down or restart the host computer.

To stop all Enterprise Manager components on a host, use the following procedure:

1. Stop the Oracle Management Service:

```
$PROMPT> $ORACLE_HOME/bin/emctl stop oms -all
```
2. Change directory to the home directory for the Oracle Management Agent and stop the Management Agent:

```
$PROMPT> AGENT_HOME/bin/emctl stop agent
```

Note

Be sure to run the `emctl stop agent` command in the Oracle Management Agent home directory and not in the Oracle Management Service home directory.

3. If your Oracle Management Repository resides on the same host, follow these steps:
 - a. Set the ORACLE_HOME environment variable to the Management Repository database home directory.
 - b. Set the ORACLE_SID environment variable to the Management Repository database SID (default is asdb).
 - c. Stop the database instance:

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

d. Stop the Net Listener:

```
$PROMPT> $ORACLE_HOME/bin/lsnrctl stop
```

Services That Are Started with Oracle Management Service Startup

When you start the Management Service, the following services are started:

1. Apache processes to start the HTTP server.
2. Node Manager Java process. This is the watchdog for the Managed Server and Admin Server processes. It restarts the Managed Server and Admin Server processes if they crash.
3. Admin Server Java process (if the command to start OMS is executed on the first OMS machine). This is the WebLogic Server instance that maintains configuration data for configured Enterprise Manager domain.
4. Managed Server Java process. This is the Managed WebLogic Server on which Enterprise Manager application is deployed.
5. *(On Windows only)* Node Manager service process. This is the Windows service for starting and stopping the Node Manager (equivalent to the Node Manager process on Linux).
6. *(On Windows only)* OMS service process. This is the Windows service for starting and stopping the OMS.

Starting and Stopping the Oracle Management Service and Management Agent on Windows

When you install the Oracle Management Service (OMS) or the Management Agent on a Windows system, the installation procedure creates new services in the Services control panel.

The procedure for accessing the Services control panel varies, depending upon the version of Microsoft Windows you are using. For example, on Windows 2000, locate the Services control panel by selecting **Settings**, then **Administrative Tools** from the **Start** menu.

Note

The `emctl` utility is available in the `bin` subdirectory of the Oracle home where you have installed the OMS or Management Agent; however, Oracle recommends that you use the Services control panel to start and stop OMS or Management Agent on Windows systems.

[Table 7-1](#) describes the Windows service that you use to control the OMS and Management Agent.

Table 7-1 Service Installed and Configured When Installing the OMS and Management Agent on Windows

Component	Service Name Format	Description
Oracle Management Server	OracleManagementServer_EMGC_OMS1_1	Use this service to start and stop all components that were installed and configured as part of the Management Service J2EE application.
Oracle Management Agent	Oracle<agent_home>Agent For example: OracleOraHome1Agent	Use this service to start and stop the Management Agent.

Reevaluating Metric Collections Using EMCTL Commands

Use the following command to perform an immediate reevaluation of a metric collection:

```
emctl control agent runCollection <targetName>:<targetType> <collectionItemName>
```

where <collectionItemName> is the name of the Collection Item that collects the metric.

Related metrics are typically collected together; collectively a set of metrics collected together is called a Metric Collection. Each Metric Collection has its own name. If you want to reevaluate a metric, you first need to determine the name of the Metric Collection to which it belongs, then the CollectionItem for that Metric Collection.

When you run the command above to reevaluate the metric, all other metrics that are part of the same Metric Collection and Collection Item will also be reevaluated.

Perform the following steps to determine the Metric Collection name and Collection Item name for a metric:

1. Go to \$INSTALL_BASE/ngagent/plugins directory, where \$INSTALL_BASE is the root of the installation. The Oracle Home of the Management Agent exists in this directory.
2. Locate the XML file for the target type. For example, if you are interested in the host metric 'Filesystem Space Available(%)' metric, look for the host.xml file.
3. In the xml file, look for the metric in which you are interested. The metric that you are familiar with is actually the display name of the metric. The metric name would be preceded by a tag that started with:

```
<Label NLSID=
```

For example, in the host.xml file, the metric 'Filesystem Space Available(%)' would have an entry that looks like this:

```
<Label NLSID="host_filesys_pctAvailable">Filesystem Space Available (%) </Label>
```

4. Once you have located the metric in the xml file, you will notice that its entry is part of a bigger entry that starts with:

```
<Metric NAME=
```

Take note of the value defined for "Metric NAME". This is the Metric Collection name. For example, for the 'Filesystem Space Available(%)' metric, the entry would look like this:

```
<Metric NAME="Filesystems"
```

So for the 'Filesystem Space Available(%)' metric, the Metric Collection name is 'Filesystems'.

5. The Collection Item name for this Metric Collection needs to be determined next. Go to the \$INSTALL_BASE/plugins/<plugin id directory, where \$INSTALL_BASE is the Oracle Home of the Management Agent.
6. In this directory, look for the collection file for the target type. In our example, this would be host.xml.
7. In cases where a Metric Collection is collected by itself, there would be a single Collection Item of the same name in the collection file. To determine if this is the case for your Metric Collection, look for an entry in the collection file that starts with:

```
<CollectionItem NAME=
```

where the value assigned to the CollectionItem NAME matches the Metric NAME in step (4).

For the 'Filesystem Space Available(%)' metric, the entry in the collection file would look like:

```
<CollectionItem NAME = "Filesystems"
```

8. If you find such an entry, then the value assigned to "CollectionItem NAME" is the collection item name that you can use in the emctl command.
9. Otherwise, this means the Metric Collection is collected with other Metric Collections under a single Collection Item. To find the Collection Item for your Metric Collection, first search for your Metric Collection. It should be preceded by the tag:

```
<MetricColl NAME=
```

Once you have located it, look in the file above it for: <CollectionItem NAME=

The value associated with the CollectionItem NAME is the name of the collection item that you should use in the emctl command.

For example if the you want to reevaluate the host metric "Open Ports", using the previous steps, you would do the following:

- a. Go to the \$INSTALL_BASE/plugins/<plugin id directory where \$INSTALL_BASE is the Oracle Home of the Management Agent. Look for the host.xml file and in that file locate: <Metric NAME="openPorts".
- b. Then go to the \$INSTALL_BASE/ngagent/plugins/default_collection directory. Look for the host.xml file and in that file look for <CollectionItem NAME="openPorts".
Failing this, look for <MetricColl NAME="openPorts".
- c. Look above this entry in the file to find the <CollectionItem NAME= string and find <CollectionItem NAME="oracle_security".

The CollectionItem NAME oracle_security is what you would use in the emctl command to reevaluate the Open Ports metric.

Specifying New Target Monitoring Credentials in Enterprise Manager

To monitor the status and performance of your database targets, Enterprise Manager connects to your database using a database user name and password. The user is referred to as the

database monitoring user; the user name and password combination is referred to as the database monitoring credentials.

When you first add, provision or clone an Oracle database target, by default Enterprise Manager uses the DBSNMP database user account and the password for the DBSNMP account as the monitoring credentials.

Alternatively, you may choose to use a different user as the database monitoring user. This new user must have the same roles and privileges as DBSNMP. To create this database monitoring user, refer to MOS note *EM 13c: Creating the Oracle Database Monitoring Credentials for Oracle Enterprise Manager 13.5 RU4 (and later)* [DocID 2847191.1](#)

non-DBSNMP Monitoring User Availability:

- *Adding an Oracle database:* Enterprise Manager 13c Release 5 Update 4 and later
- *Database-as-a-Service:* Enterprise Manager 13c Release 5 Update 8 and later
- *Oracle database provisioning (outside Exadata) and cloning:* Enterprise Manager 13c Release 5 Update 8 and later
- *Oracle database provisioning for Exadata:* Enterprise Manager 13c Release 5 Update 9 and later

Notes:

While discovery and monitoring of Oracle database targets works with non-DBSNMP users, there are management features that still assume DBSNMP as the database monitoring user.

These features include the following:

- Oracle Database Benchmarks such as CIS Oracle Database 19c Benchmark include assessments for the DBSNMP user. These assessments will continue to support only the DBSNMP user, and not other database users used as monitoring credentials
- For monitoring AVDF (Oracle Audit Vault and Database Firewall) targets, the use of non-DBSNMP users as monitoring credentials is not supported.

EMCTL Commands for OMS

[Table 7-2](#) lists the EMCTL commands for OMS.

Table 7-2 EMCTL Commands for OMS

EMCTL Command	Description
<code>emctl getversion oms</code>	Shows the version of the OMS instance.
<code>emctl start oms</code>	Starts the Fusion Middleware components required to run the OMS application and the JVM engine. Specifically, this command starts HTTP Server, the Node Manager, and the managed server on which the Management Service is deployed. In addition, if this command is run on the host that has the Administration Server, then the Administration Server is also started. Note: Only the Oracle software owner can start or stop the OMS.
<code>emctl start oms - admin_only</code>	Starts only the Administration Server of the domain.

Table 7-2 (Cont.) EMCTL Commands for OMS

EMCTL Command	Description
<code>emctl stop oms</code>	Stops the OMS managed server and JVM engine, but leaves HTTP server, Node Manager and Administration Server running. Note: The <code>emctl stop oms</code> command does not stop Fusion Middleware.
<code>emctl stop oms -all</code>	Stops all Enterprise Manager processes including Administration Server, OMS, HTTP Server, Node Manager, Management Server, and JVM engine.
<code>emctl stop oms -all -force</code> and <code>emctl stop oms -force</code>	Stops the OMS. The parameter <code>-force</code> can be used with both <code>emctl stop oms -all</code> and <code>emctl stop oms</code> commands. The <code>-force</code> option forcefully stops the relevant processes. Using this parameter is not recommended.
<code>emctl status oms</code>	Lists the statuses of the OMS and JVM engine.
<code>emctl status oms -details [-sysman_pwd <pwd>]</code>	Lists the OMS details such as: <ul style="list-style-type: none"> • HTTP and HTTPS upload and console ports of the OMS and the respective URLs • Instance home location • OMS log directory • Software Load Balancer configuration details • Administration server machine and port • JVM engine The <code>-sysman_pwd</code> parameter indicates the Enterprise Manager SYSMAN password. If it is not provided on the command line, you will be prompted for it.
<code>emctl set property</code>	Sets the values of the OMS configuration properties. By default, the command <code>emctl set property</code> will set the property value for all the OMSs. To set the property value for a specific OMS, specify an extra option <code>-oms_name</code> , which should be in the format <code>hostname.myco.com:17707_Management_Service</code> . To set the property value for the current OMS, specify <code>-oms_name = "local_oms."</code> . To set the property for a remote OMS, specify <code>-oms_name=<name of remote OMS></code> . Note: You can also view and edit OMS properties from the Enterprise Manager console as follows: <ol style="list-style-type: none"> 1. From the Setup menu, select Manage Enterprise Manager, then select Management Services. 2. On the Management Services page, click Configuration Properties. 3. On the Configuration Properties page, you can view and edit OMS properties. Note: You will need OMS Configuration Property resource privilege to navigate to this page.
<code>emctl get property</code>	Displays the values of OMS configuration properties.
<code>emctl get property -name <property name> [-oms_name <OMS name>] [-sysman_pwd "sysman password"]</code>	Displays the value of the specified property. <code>-name</code> indicates the name of the property and <code>-oms_name</code> indicates the name of the OMS for which the property value is to be derived. If <code>-oms_name</code> is not mentioned, the property value for all the OMSs are displayed.

Table 7-2 (Cont.) EMCTL Commands for OMS

EMCTL Command	Description
<pre>emctl set property -name <property name> -value <property value> [- oms_name <OMS name>] [- module <emoms logging>] [- sysman_pwd "sysman password"]</pre>	<p>Sets the value of the specified property.</p> <p>The parameters are explained below:</p> <ul style="list-style-type: none"> • <code>-name</code>: Indicates the name of the property. • <code>-oms_name</code>: Indicates the OMS for which the property value has to be set. In case this option is not specified, the property value is set at a global level or for the current OMS. • <code>-module_name</code>: Indicates the module for the property. Specify either <code>logging</code> or <code>emoms</code>. Logging properties are used to configure Log4j whereas <code>emoms</code> properties are used to configure the OMS.
<pre>emctl set property -file <absolute path of the file containing properties> [-oms_name <OMS name>] [-module <emoms logging>] [- sysman_pwd "sysman password"]</pre>	<p>Sets the values of the properties in the specified file.</p> <p>The parameters are explained below:</p> <ul style="list-style-type: none"> • <code>-file_name</code>: Indicates the absolute path of the <code>.properties</code> file containing the properties and the values. This file should contain only those properties whose values need to be set. • <code>-oms_name</code>: Indicates the OMS for which the property values has to be set. In case this option is not specified, the property values are set at a global level or for the current OMS. • <code>-module_name</code>: Indicates the module for the property. Specify either <code>logging</code> or <code>emoms</code>. Logging properties are used to configure Log4j whereas <code>emoms</code> properties are used to configure the OMS.
<pre>emctl delete property - name <property name> [- oms_name <OMS name>] [- module <emoms logging>] [- sysman_pwd "sysman password"]</pre>	<p>Deletes the configured value of the specified property and sets it to the default value.</p> <p><code>-name</code> indicates the name of the property and <code>-oms_name</code> indicates the name of the OMS for which the property value is to be deleted. If <code>-oms_name</code> is not mentioned, the property value is deleted at the global level or for the current OMS.</p>
<pre>emctl list properties</pre>	<p>Displays the properties of all OMSs.</p> <p>Use <code>-out_file</code> parameter to get a list of all the properties for all OMSs. This command enables easy comparison of configuration across two OMSs.</p>
<pre>emctl list properties [- oms_name <OMS name>] [- module <emoms logging>] [- out_file <output file name>] [-sysman_pwd "sysman password"]</pre>	<p>Displays the values of all the customer visible OMS properties.</p> <p>The parameters are explained below:</p> <ul style="list-style-type: none"> • <code>-oms_name</code>: Indicates the OMS for which the property values are to be displayed. In case this option is not specified, the property values for all the OMSs are displayed. • <code>-module_name</code>: Indicates the module of the properties. This option can be used as a filter to display module-specific properties. Logging properties are used to configure Log4j whereas <code>emoms</code> properties are used to configure the OMS. • <code>-out_file</code>: Indicates the absolute path of the output file. This is an optional parameter to save the output in a file.
<pre>emctl config oms - list_repos_details</pre>	<p>Displays the OMS repository details.</p>

Table 7-2 (Cont.) EMCTL Commands for OMS

EMCTL Command	Description
<pre>emctl config oms - store_repos_details [- repos_host <host> - repos_port <port> - repos_sid <sid> - repos_connndesc <connect descriptor>] - repos_user <username> [- repos_pwd <pwd>]</pre>	<p>Configures the OMS to use the specified database as the Management Repository.</p> <p>All the additional parameters mentioned in the command need to be specified.</p>
<pre>emctl config oms - change_repos_pwd [- old_pwd <old_pwd>] [- new_pwd <new_pwd>] [- use_sys_pwd [-sys_pwd <sys_pwd>]]</pre>	<p>Changes the password of root user (SYSMAN) in the repository database and in the OMS.</p> <p>To change the Enterprise Manager root user (SYSMAN) password:</p> <ol style="list-style-type: none"> 1. Stop all the OMSs using <code>emctl stop oms</code> command. 2. Run <code>emctl config oms -change_repos_pwd</code> on one of the OMSs. 3. Restart all the OMSs using the <code>emctl stop oms -all</code> and <code>emctl start oms</code> commands.
<pre>emctl config oms - change_view_user_pwd [- sysman_pwd <sysman_pwd>] [-user_pwd <user_pwd>] [-auto_generate]</pre>	<p>Configures the password used by OMS for MGMT_VIEW user that is used for report generation.</p> <p>To change the Enterprise Manager MGMT_VIEW user password:</p> <ol style="list-style-type: none"> 1. Stop all the OMSs using <code>emctl stop oms</code> command. 2. Run <code>emctl config oms -change_view_user_pwd</code> on all OMSes. 3. Restart all the OMSes using the <code>emctl stop oms -all</code> and <code>emctl start oms</code> commands.
<code>emctl secure oms</code>	Sets up the SSL configuration for OMS.
<pre>emctl genreport oms - file_name <file_name> [- dest_dir <dest_dir>]</pre>	<p>Generates and saves the emcli tracing performance report.</p> <p>-file_name indicates the name of the input file containing the trace data and -dest_dir indicates the name of the output directory where the performance report is saved.</p>
<pre>emctl gen_ui_trace_report oms [-start_time <start_time in hh:mm:ss format>] [- duration <duration in hh:mm format>] [- user_name <username>] [- out_file <out_file>] [- sysman_pwd <sysman_pwd>]</pre>	<p>Generates the performance report for user interface (UI) access.</p> <p>The parameters are explained below:</p> <ul style="list-style-type: none"> • -user_name: Indicates the user name for which the UI access performance report has to be generated. The default is for all users. • -start_time: Indicates the start time in hh:mm:ss format from when the report has to be generated. • -duration: Indicates the duration in hh:mm format for which report has to be generated. The default is 01:00. The maximum duration is limited to 24:00. • -out_file: Indicates the name of the output report file.

Table 7-2 (Cont.) EMCTL Commands for OMS

EMCTL Command	Description
emctl config oms - set_startup_mode [pbs_only console_only normal]	Configures the startup mode of the OMS. This command cannot be executed on the primary OMS. The three startup modes are as below: <ul style="list-style-type: none"> • pbs_only: If the startup mode is configured to pbs_only, then the command emctl start oms starts only the PBS application. • console_only: If the startup mode is configured to console_only, then the command emctl start oms starts only the console application. • normal: If the startup mode is configured to normal, then the command emctl start oms starts both the PBS application and the console application.
emctl config oms - get_startup_mode	Displays the OMS startup mode of the current OMS.
emctl config oms sso - host ssoHost -port ssoPort -sid ssoSid - pass ssoPassword -das dasURL -u user	Configures Enterprise Manager (EM) to use Oracle SSO (OSSO) for authentication. To run this command you should have registered the EM site with the OSSO server, as you will need the generated registration file as an input for this command.
emctl config oms - update_ds_pwd -ds_name <datasource_name> [- ds_pwd <datasource_pwd>]	Updates a new password for the specified datasource. In the command, -ds_name indicates the name of the datasource, and -ds_pwd indicates the new password of the datasource.
emctl extended oms <verb> [verb_args] [- help]	Executes the <verb> registered with the EMCTL extended framework. The verb_args parameter specifies the verb-specific arguments. The -help parameter provides the verb specific help. For a list of extended verbs, run emctl extended oms .
emctl register oms metadata -service <Metadata Service Id> (- file <Metadata Instance file> -file_list <File containing list of files to register>) (-core - pluginId <Plugin Id>)[- sysman_pwd <sysman password>]	Registers the metadata. The -file_list parameter provides the path to the file containing a list of the file paths (one on each line). These file paths are relative to OMS Oracle home or Plug-in Oracle home depending on whether the -core parameter is passed or the -pluginId parameter is passed.
emctl register oms metadata -service targetType -file <XML filename> [-core - pluginId <Plugin Id>] [- sysman_pwd "sysman password"] and emctl register oms metadata - service storeTargetType -file <XML filename> [- core -pluginId <Plugin Id>] [-sysman_pwd "sysman password"]	Registers a target type when these two commands are executed, one after the other. The parameter -file <XML filename> specifies the target type .xml file name with the absolute path or the relative path.

Table 7-2 (Cont.) EMCTL Commands for OMS

EMCTL Command	Description
<pre>emctl deregister oms metadata -service <Metadata Service Id> (- file <Metadata Instance file> && (-old_file <File containing previous metadata instances> - no_old_file <in case there are no previous metadata instances>)) -file_list <File containing list of ';' separated new and old files to deregister> (- core -pluginId <Plugin Id>) [-sysman_pwd <sysman password>]</pre>	<p>Erases the metadata.</p> <p>The <code>-file_list</code> option provides the path to the file containing the list of file paths (one on each line). These file paths are relative to OMS Oracle home or Plug-in Oracle home depending on whether the <code>-core</code> parameter is passed or the <code>-pluginId</code> parameter is passed.</p>

EMCTL Commands for Management Agent

[Table 7-3](#) lists the EMCTL commands for Management Agents.

Table 7-3 EMCTL Commands for Management Agent

EMCTL Command	Description
emctl start agent	<p>Starts the Management Agent.</p> <p>On IBM AIX environment with a large memory configuration where the Management Agent is monitoring a large number of targets, the Agent may not start. To prevent this issue, prior to starting the Management Agent, add the following parameters to the common environment file:</p> <pre>LDR_CNTRL="MAXDATA=0x80000000"@NOKRTL AIXTHREAD_SCOPE=S</pre> <p>The <code>LDR_CNTRL</code> variable sets the data segment size and disables loading of run time libraries in kernel space. The <code>AIXTHREAD_SCOPE</code> parameter changes AIX Threadscope context from the default Processwide 'P' to Systemwide 'S'. This causes less mutex contention.</p>
emctl stop agent	Stops the Management Agent.
emctl status agent	<p>Lists the status of Management Agent.</p> <p>If the Management Agent is running, this command displays status information about the Management Agent, including the Agent Home, the process ID, and the time and date of the last successful upload to the Management Repository ().</p> <p>Note: On a Windows system change the directory to the <code>AGENT_INSTANCE_HOME</code> directory before executing the command.</p>
emctl status agent -secure	Lists the secure status of the Management Agent and the secure mode port on which the Management Agent is running. It also lists the OMS security status and the port.

Table 7-3 (Cont.) EMCTL Commands for Management Agent

EMCTL Command	Description
<code>emctl status agent scheduler</code>	Lists all the running, ready, and scheduled collection threads.
<code>emctl status agent jobs</code>	Lists the status of the jobs that are running at present on the Management Agent.
<code>emctl status agent target <target name>, <target type>, <metric></code>	Lists the detailed status of the specified targets such as target name, target type, and so on. You can also provide a particular metric name in the <code>emctl status agent</code> command to get the status of a particular metric of a target.
<code>emctl status agent mcache <target name>, <target type>, <metric></code>	Lists the names of the metrics whose values are present in the metric cache.
<code>emctl upload</code>	Uploads the .xml files that are pending to the OMS under the upload directory.
<code>emctl upload (agent)</code>	Use this command to force an immediate upload of the current management data from the managed host to the Management Service. Use this command instead of waiting until the next scheduled upload of the data.
<code>emctl reload (agent)</code>	<p>This command can be used to apply the changes after you have manually modified the <code>emd.properties</code> file. For example, to change the upload interval, <code>emd.properties</code> can be modified, and <code>emctl reload</code> can then be run.</p> <p>Note: Oracle does not support manual editing of the <code>targets.xml</code> files unless the procedure is explicitly documented or you are instructed to do so by Oracle Support.</p>
<code>emctl reload agent dynamicproperties [<Target_name>:<Target_Type>]...</code>	Recomputes the dynamic properties of a target and displays them.
<code>emctl pingOMS [agent]</code>	Pings the OMS to check if the Management Agent is able to connect to the OMS. Management Agent will wait for the reverse ping from the OMS so that Management Agent can confirm that the <code>pingOMS</code> is successful.
<code>emctl config agent getTZ</code>	Configures the current time zone as set in the environment.
<code>emctl config agent getSupportedTZ</code>	Displays the supported time zone based on the setting in the environment.
<code>emctl config console <fileloc> [<EM loc>]</code>	<p>Configures the console based on the configuration entries mentioned in the file <code><fileloc></code>.</p> <p>The <code><EM loc></code> parameter is optional and can be used to operate on a different Oracle home.</p>
<code>emctl config agent listtargets [<EM loc>]</code>	<p>Lists all the target names and types monitored by the Management Agent, that are present in <code>targets.xml</code> file.</p> <p>The <code><EM loc></code> parameter is optional and can be used to operate on a different Oracle home.</p>

Table 7-3 (Cont.) EMCTL Commands for Management Agent

EMCTL Command	Description
emctl control agent runCollection <target_name>:<target_type> <metric_name>	Allows you to manually run the collections for a particular metric of a target. For example, <code>emctl control agent runCollection myOracleHomeTargetName:oracle_home oracle_home_config.</code>
emctl control agent runCollection <targetName>:<targetType> > <collectionItemName>	Performs an immediate reevaluation of a metric collection Executing this command causes the reevaluated value of the metric to be uploaded into the Management Repository, and possibly trigger alerts if the metric crosses its threshold. To identify the metric name and the collection item name associated with the metric, see Reevaluating Metric Collections Using EMCTL Commands .
emctl resetTZ agent	Resets the time zone of the Management Agent. To change the current time zone to a different time zone, stop the Management Agent and then run this command. You can then start the Management Agent. Important: Before you change the Management Agent time zone, first check to see if there are any blackouts that are currently running or scheduled to run on any targets managed by that Management Agent. Refer to Viewing Blackouts/Notification Blackouts to know how to check for blackouts. If any blackouts exist, then from the Enterprise Manager console, stop all the scheduled and all the currently running blackouts on all targets monitored by that Management Agent. You can then change the Management Agent's time zone and later create new blackouts on the targets as needed.
emctl getversion agent	Prints the version of the Management Agent.
emctl dumpstate agent <component> . . .	Generates the dumps for the Management Agent. This command allows you to analyze the memory/CPU issues of the Management Agent.
emctl gensudoprops	Generates the sudo properties of the Management Agent.
emctl clearsudoprops	Clears the sudo properties.
emctl clearstate	Clears the state directory contents. The files that are located in the <code>\$ORACLE_HOME/sysman/emd/state</code> will be deleted if this command is run. The state files are the files which are waiting for the Management Agent to convert them into corresponding <code>.xml</code> files.
emctl getemhome	Prints the Management Agent home directory.
emctl start blackout <Blackoutname> [- nodeLevel] [<Target_name>[:<Target_ Type>]]... [-d <Duration>]	Starts blackout on a target. If the parameter <code><Target_name:Target_type></code> is not entered, then the local node target is taken as the default. If <code>-nodeLevel</code> parameter is specified after <code><Blackoutname></code> , the blackout will be applied to all targets and any target list that follows will be ignored. The <code><Duration></code> should be specified in <code>[days] hh:mm</code> format.
emctl stop blackout <Blackoutname>	Stops the blackout that was started on a particular target. Only those blackouts that are started by the <code>emctl</code> tool can be stopped using <code>emctl</code> . This command cannot stop the blackouts that are started using the console or <code>em cli</code> utility.

Table 7-3 (Cont.) EMCTL Commands for Management Agent

EMCTL Command	Description
emctl status blackout [<Target_name>[:<Target_Type>]]....	Provides the status of the target blackout. The status includes the type of blackout and whether it is a one-time action, or repeating, or a scheduled blackout. This command also specifies whether the blackout has started or stopped.
emctl secure agent [registration password] -emdWalletSrcUrl <url> - protocol <ssl tls>	<p>Secures the Management Agent with an OMS. The registration password is essential, as you will be prompted for it if you do not provide it along with the command.</p> <p>The -emdWalletSrcUrl parameter indicates the URL of the OMS with which the agent has to be secured.</p> <p>The -protocol parameter indicates the protocol to be used to secure the Management Agent. The allowed values are <code>ssl</code> and <code>tls</code>.</p>
emctl unsecure agent	Un-secures the Management Agent. This command changes the Management Agent's port to a HTTP port. After executing this command the Management Agent will be able to upload to the OMS on HTTP by connecting to OMS's HTTP upload port instead of the HTTPS upload port.
emctl verifykey	Verifies the communication between the OMS and Management Agent by sending pingOMS.
emctl deploy agent [-s <install-password>] [-o <omshostname:consoleSrvPort>] [-S] <deploy-dir> <deploy-hostname>:<port> <source-hostname>	<p>Creates and deploys only the Management Agent.</p> <p>The parameters are explained below:</p> <ul style="list-style-type: none"> [-s <password>]: Indicates the install password for securing the Management Agent. [-S]: Indicates that the password will be provided in STDIN. [-o <omshostname:consoleSrvPort>]: Indicates the OMS host name and the console servlet port. Choose the un-secured port. <deploy-dir>: Indicates the directory to create the shared (state-only) installation port. <deploy-hostname:port>: Indicates the host name and the port of the shared (state-only) installation. Choose an unused port. <source-hostname>: Indicates the host name of the source install. Typically, it is the machine where the EM is installed. The host name is searched for and replaced in the <code>targets.xml</code> file with the host name provided in the argument <code><deploy-hostname:port></code>. <sid>: Indicates the instance of the remote database. It is only specified when deploying the <code>dbconsole</code>.

Table 7-3 (Cont.) EMCTL Commands for Management Agent

EMCTL Command	Description
emctl setproperty agent	<p>Configures the specified property name and value in the Management Agent configuration file. The flag, <code>allow_new</code> is an optional flag that inserts a new property in the Management Agent configuration file, if it does not exist.</p> <p>Pattern Matching Behavior</p> <p>When key column conditions are created, the agent evaluates these conditions against rows even when the expression only matches a portion of the value. For example, a <i>condition</i> defined against <code>/ul%</code> may be applied against <code>/prod/ulz</code> Note: Customers who prefer the previous behavior have the option of setting the property <code>"_KeyColumnLikeMatchesSubstring"</code> to <code>TRUE</code></p> <pre>emctl setproperty agent -allow_new -name _KeyColumnLikeMatchesSubstring -value TRUE</pre>
emctl getproperty agent	Gets the specified properties or a category of properties from the Management Agent configuration files. Currently, this command does not support spaces in the name. The flag, <code>-name</code> provides a list of property names separated by spaces.
emctl clear_property agent	Clears the value of the specified property in the Management Agent configuration file.
emctl status agent verify	Verifies that the Management Agent is live.

EMCTL Security Commands

This section explains the EMCTL security commands.

The topics covered in this section are:

- [EMCTL Secure Commands](#)
- [Security diagnostic commands](#)
- [EMCTL EM Key Commands](#)
- [Configuring Authentication](#)

EMCTL Secure Commands

[Table 7-6](#) lists the general EMCTL security commands.

Table 7-4 EMCTL Secure Commands

EMCTL Command	Description
emctl secure console [-sysman_pwd <pwd>] (-wallet <wallet_loc> -self_signed) [-key_strength <strength>] [-cert_validity <validity>]	Sets up the SSL configuration for the HTTPS console port of the OMS.
emctl secure lock [-sysman_pwd <pwd>] [-console] [-upload]	<p>Locks the OMS upload and console, thereby avoiding HTTP access to the OMS.</p> <p>The -console and -upload parameters are optional.</p> <p>The -console parameter locks and prevents HTTP access to the EM console, in which case, the EM console can be accessed only over HTTPS.</p> <p>The -upload parameter prevents the Management Agents from uploading data to the OMS over HTTP, due to which the Management Agents can connect to the OMS only over HTTPS.</p>
emctl secure unlock [-sysman_pwd <pwd>] [-console] [-upload]	<p>Unlocks the OMS upload and console thereby allowing HTTP access to the OMS.</p> <p>The -console and -upload parameters are optional.</p> <p>The -console parameter unlocks the console for access over HTTP as well.</p> <p>The -upload parameter unlocks the upload activity thereby allowing the Management Agents to upload data to the OMS over HTTP as well.</p>
emctl secure createca [-sysman_pwd <pwd>] [-root_country <root_country>] [-root_state <root_state>] [-root_org <root_org>] [-root_unit <root_unit>] [-key_strength <strength>] [-cert_validity <validity>]	Creates a new Certificate Authority (CA) which is used to issue certificates during subsequent securing of OMS and Management Agents.
emctl secure setpwd [sysman password] [new registration password]	Adds a new Management Agent registration password.
emctl secure sync	Verifies if the Management Repository is up.
emctl secure create_admin_credentials [-admin_pwd <pwd>] [-nodemgr_pwd <pwd>]	Re-creates the Administrator Credentials wallet.

Table 7-4 (Cont.) EMCTL Secure Commands

EMCTL Command	Description
<pre>emctl secure oms [- sysman_pwd <sysman password>] [-reg_pwd <registration password>] [-host <hostname>] [- ms_hostname <Managed Server hostname>] [slb_port <SLB HTTPS upload port>] [- slb_console_port <SLB HTTPS console port>] [- no_slb] [-secure_port <OHS HTTPS upload Port>] [-upload_http_port <OHS HTTP upload port>] [- reset] [-console] [- force_newca] [- lock_upload] [- lock_console] [- unlock_upload] [- unlock_console] [-wallet <wallet_loc> - trust_certs_loc <certs_loc>] [- key_strength <strength>] [-sign_alg <md5 sha1 sha256 sha384 sha512>] [-cert_validity <validity>] [-protocol <protocol>] [-root_dc <root_dc>] [- root_country <root_country>] [- root_email <root_email>] [-root_state <root_state>] [-root_loc <root_loc>] [-root_org <root_org>] [-root_unit <root_unit>]</pre>	<p>The <code>emctl secure oms</code> command generates a root key within the Management Repository, modifies the WebTier to enable an HTTPS channel between the OMS and Management Agents, and enables the OMS to accept requests from the Management Agents using the Enterprise Manager Framework Security.</p>
<pre>emctl secure wls [- sysman_pwd <sysman password>] [-jks_loc <loc> -jks_pvtkey_alias <alias> -wallet <loc> -use_demo_cert)</pre>	<p>The <code>emctl secure wls</code> command secures the WebLogic Server.</p>

The parameter descriptions for the above commands are explained below.

- `-host`: Indicates the Software Load Balancer (SLB) or virtual host name.
- `-ms_hostname`: Indicates the actual host name of the machine where the OMS is running.
- `-slb_port`: Indicates the HTTPS port configured on SLB for uploads.

- `-slb_console_port`: Indicates the HTTPS port configured on SLB for console access.
- `-no_slb`: Removes the SLB configuration.
- `-secure_port` : Specifies the HTTPS upload port change on WebTier.
- `-upload_http_port`: Specifies the HTTP upload port change on WebTier.
- `-reset`: Creates new CA.
- `-force_newca`: Forces OMS to secure with the new CA, even when there are Management Agents secured with the older CA.
- `-console`: Creates a certificate for console HTTPS port as well.
- `-lock_upload`: Locks upload.
- `-lock_console`: Locks console.
- `-unlock_upload`: Unlocks upload.
- `-unlock_console`: Unlocks console.
- `-wallet`: Indicates the directory where the external wallet is located.
- `-trust_certs_loc`: Indicates the file containing all the trusted certificates.
- `-key_strength`: 512|1024|2048
- `-sign_alg`: Signature Algorithm; md5|sha1|sha256|sha384|sha512.
- `-cert_validity`: Indicates the number of days the certificate should be valid. The minimum value is 1 and the maximum value is 3650.
- `-protocol`: Indicates the SSL protocol to be used on WebTier. The valid values for `<protocol>` are the allowed values for Apache's SSL protocol directive.
- `-jks_loc`: Indicates the location of JKS containing the custom certificate for administrator and managed servers.
- `-jks_pvtkey_alias`: Indicates the JKS private key alias.
- `-jks_pwd`: Indicates the JKS key store password.
- `-jks_pvtkey_pwd`: Indicates the JKS private key password.
- `-wallet`: Indicates the location of the wallet containing the custom certificate for administrator and managed servers.
- `-use_demo_cert`: Configures the demonstration certificate for administrator and managed servers.

Security diagnostic commands

[Table 7-5](#) lists the EMCTL security diagnostic commands.

Table 7-5 EMCTL Security Diagnostic Commands

EMCTL Command	Description
emctl secdiag openurl -url <url> [-trust_store <location of jks or base64 file>] [-ssl_protocol <protocol>] [-cipher <low medium high some_ciphersuite_name>] [-proxy_host <host> -proxy_port <port>] [-proxy_realm <realm>] [-proxy_user <user> -proxy_pwd <pwd>]	<p>Diagnoses the connectivity issues to the specified URL.</p> <p>The parameter descriptions are as follows:</p> <ul style="list-style-type: none"> • -url: Indicates the URL to be tested. • -trust_store: Indicates the location of the trust store. It can be a jks or base64 file. If it is not specified, the connection will be blindly trusted. • -ssl_protocol: Indicates the protocol to be used to make the connection. • -cipher: Indicates the cipher suites to be used. You can specify low, medium, high or a cipher suite name. • -proxy_host: Indicates the host name of the proxy server. • -proxy_port: Indicates the proxy server's port number. • -proxy_realm: Indicates the proxy server's realm. • -proxy_user: Indicates the proxy user ID. • -proxy_password: Indicates the proxy user password.
emctl secdiag dumpcertsinrepos -repos_connndesc <connect descriptor> [-repos_pwd <pwd>]	Displays the trust certificates stored in the specified repository.
emctl secdiag dumpcertsinfile -file <location of jks/sso/p12/base64 file>	Displays the trust certificates present in the specified key store, or wallet, or base64 file.

EMCTL EM Key Commands

[Table 7-6](#) lists the EMCTL EM Key commands.

Table 7-6 EMCTL EM Key Commands

EMCTL Command	Description
emctl status emkey [-sysman_pwd <pwd>]	Displays the health or status of the emkey.
emctl config emkey -copy_to_credstore [-sysman_pwd <pwd>]	Copies the emkey from the Management Repository to the Credential Store.
emctl config emkey -remove_from_repos [-sysman_pwd <pwd>]	Removes the emkey from the Management Repository.

Table 7-6 (Cont.) EMCTL EM Key Commands

EMCTL Command	Description
emctl config emkey - copy_to_file_from_credstore -admin_host <host> - admin_port <port> - admin_user <username> [- admin_pwd <pwd>] [- repos_pwd <pwd>] - emkey_file <emkey file>	Copies the emkey from the Credential Store to the specified file.
emctl config emkey - copy_to_file_from_repos (-repos_host <host> - repos_port <port> - repos_sid <sid> - repos_conn_desc <conn desc>) -repos_user <username> [-repos_pwd <pwd>] [-admin_pwd <pwd>] -emkey_file <emkey file>	Copies the emkey from the Management Repository to the specified file.
emctl config emkey - copy_to_credstore_from_file -admin_host <host> - admin_port <port> - admin_user <username> [- admin_pwd <pwd>] [- repos_pwd <pwd>] - emkey_file <emkey file>	Copies the emkey from the specified file to the credential store.
emctl config emkey - copy_to_repos_from_file (-repos_host <host> - repos_port <port> - repos_sid <sid> - repos_conn_desc <conn desc>) -repos_user <username> [-repos_pwd <pwd>] [-admin_pwd <pwd>] -emkey_file <emkey file>	Copies the emkey from the specified file to the Management Repository.

Configuring Authentication

This section explains the EMCTL commands for configuring authentications.

The commands covered in this section are:

- [Configuring OSSO Authentication](#)
- [Configuring OAM Authentication](#)
- [Configuring LDAP \(OID and AD\) Authentication](#)
- [Configuring Repository Authentication \(Default Authentication\)](#)

The parameter descriptions for all these commands are as below:

- `-enable_auto_provisioning`: Enables automatic-provisioning in EM, wherein external LDAP users need not be provisioned manually in EM.
- `-auto_provisioning_minimum_role <min_role>`: Automatically provisions only those external users in EM who have the `min_role` granted to them in LDAP.
- `-minimum_privilege <min_priv>`: Prevents access to EM to users who do not have the `min_priv` granted to them.
- `-use_ssl`: Indicates the SSL to connect to the LDAP server.
- `-cert_file <cert>`: Indicates the LDAP server certificate to establish trust while connecting to LDAP server over SSL. Specify this option if the LDAP server has the certificate signed by a non-popular (or non-trusted) certificate authority.

Note

This parameter accepts only a single certificate. Importing certificate chains is not supported. Import the certificate using `keytool` utility before running this command.

- `-trust_cacerts`: Establishes trust to the LDAP server's certificate while connecting to the LDAP server. This parameter is typically used if the certificate is signed by a well known certificate authority.
- `-keystore_pwd <passwd>`: Indicates the password for the default `DemoTrust.jks` keystore (if the default password has changed), or any custom keystore to which the LDAP server's certificate will be imported as a part of validation.
- `-use_anonymous_bind`: Uses anonymous bind to connect to LDAP server.

Configuring OSSO Authentication

EMCTL OSSO authentication command configures the Enterprise Manager to use the Oracle Application Server Single Sign-On to register any single sign-on user as an Enterprise Manager administrator. The EMCTL command to configure OSSO authentication is:

```
emctl config auth sso -ossoconf <conf file loc> -dasurl <DAS URL> [-unsecure] [-sysman_pwd <pwd>] [-domain <domain>] -ldap_host <ldap host> -ldap_port <ldap port> -ldap_principal <ldap principal> [-ldap_credential <ldap credential>] -user_base_dn <user base DN> -group_base_dn <group base DN> [-logout_url <sso logout url>] [-enable_auto_provisioning] [-auto_provisioning_minimum_role <min_role>] [-minimum_privilege <min_priv>] [-use_ssl] [-cert_file <cert>] [-trust_cacerts] [-use_anonymous_bind] [-keystore_pwd <passwd>]
```

For example, `emctl config auth sso -ossoconf $T_WORK/osso.conf -dasurl "http://xxx.oracle.com:11" -sysman_pwd sysman -ldap_host xxx.oracle.com -ldap_port 111 -ldap_principal cn=orcladmin -ldap_credential ackdele1 -user_base_dn "cn=Users,dc=us,dc=oracle,dc=com" -group_base_dn "cn=Groups,dc=us,dc=oracle,dc=com" -logout_url "http://xxx.oracle.com:11/pls/orasso/orasso.wwsso_app_admin.ls_logout?p_done_url=https://xyy.oracle.com:216/em.`

Configuring OAM Authentication

Oracle Access Manager authentication is the Oracle Fusion Middleware single sign-on solution. This authentication scheme is used for data centers that have standardized on Oracle Access Manager as the central tool for authentication across all enterprise applications. The EMCTL command to configure OAM authentication is:

```
emctl config auth oam [-sysman_pwd <pwd>] -oid_host <host> -oid_port <port> -
oid_principal <principal> [-oid_credential <credential>] [-use_anonymous_bind] -
user_base_dn <dn> -group_base_dn <dn> -oam_host <host> -oam_port <port> [-
logout_url <url>] [-is_oamlog] [-user_dn <dn>] [-group_dn <dn>] [-
enable_auto_provisioning] [-auto_provisioning_minimum_role <min_role>] [-
minimum_privilege <min_priv>] [-use_ssl] [-cert_file <cert>] [-trust_cacerts] [-
keystore_pwd <passwd>]
```

For example, `emctl config auth oam -oid_host "xxx.oracle.com" -oid_port "111" -oid_principal "cn=orcladmin" -user_base_dn "cn=users,dc=us,dc=oracle,dc=com" -group_base_dn "cn=groups,dc=us,dc=oracle,dc=com" -oam_host "xxx.oracle.com" -oam_port "555" -oid_credential "eldlecol" -sysman_pwd "sysman" -logout_url http://xxx.oracle.com:23716/oam/server/logout?end_url=https://yyy.oracle.com:5416/em -enable_auto_provisioning -auto_provisioning_minimum_role "EM_DBA"`.

Configuring LDAP (OID and AD) Authentication

The EMCTL command for configuring OID authentication is as below. For AD, replace the command syntax `emctl config auth oid` below with `emctl config auth ad`. All other parameters remain the same.

OID authentication command configures the Oracle Internet Directory as the identity store for all the applications to authenticate its users against the OID.

Similarly, AD authentication command configures the Microsoft Active Directory as the identity store for all the applications to authenticate its users against the AD.

```
emctl config auth oid -ldap_host <ldap host> -ldap_port <ldap port> -
ldap_principal <ldap principal> [-ldap_credential <ldap credential>] [-sysman_pwd
<pwd>] -user_base_dn <user base DN> -group_base_dn <group base DN> [-user_dn
<dn>] [-group_dn <dn>] [-enable_auto_provisioning] [-
auto_provisioning_minimum_role <min_role>] [-minimum_privilege <min_priv>] [-
use_ssl] [-cert_file <cert>] [-trust_cacerts] [-use_anonymous_bind] [-
keystore_pwd <passwd>]
```

For example, `emctl config auth oid -ldap_host "xxx.oracle.com" -ldap_port "111" -ldap_principal "cn=orcladmin" -user_base_dn "cn=users,dc=us,dc=oracle,dc=com" -group_base_dn "cn=groups,dc=us,dc=oracle,dc=com" -ldap_credential "elecmeel" -sysman_pwd "sysman" -use_ssl -cert_file "/scratch/oidcert.txt"`.

Configuring Repository Authentication (Default Authentication)

The repository authentication command validates the user credentials against the Management Repository for authentication. The EMCTL command to configure the repository authentication is:

```
emctl config auth repos [-sysman_pwd <pwd>]
```

EMCTL HAConfig Commands

[Table 7-7](#) lists the EMCTL HA configuration commands.

Table 7-7 EMCTL HA Configuration Commands

EMCTL Commands	Description
<pre>emctl exportconfig oms [-sysman_pwd <sysman password>]</pre>	<p>Exports a snapshot of the OMS configuration to the specified directory. It is recommended to save the configuration details in a secure location and to save it every time there is a change in the configuration. These details will be required during a system recovery.</p> <p>The parameter descriptions are as below:</p> <ul style="list-style-type: none"> • <code>-oms_only</code>: Specifies the OMS-only backup on Administration server host. • <code>-keep_host</code>: Specifies that the host name will also be a part of the backup if no SLB is defined. Use this option only if recovery will be done on a machine that responds to this host name.
<pre>emctl importconfig oms - file <backup file> [- no_resecure] [- sysman_pwd <sysman password>] [-reg_pwd <registration password>]</pre>	<p>Imports the OMS configuration from the specified backup file. This command is used during a system recovery. The parameter descriptions are as below:</p> <ul style="list-style-type: none"> • <code>-file <backup file></code>: Indicates the backup file to import from. • <code>-no_resecure</code>: Specifies that the system will not re-secure OMS after the import is complete. The default is to re-secure the OMS after the import is complete.
<pre>emctl config emrep [- sysman_pwd <sysman password>]</pre>	<p>Configures the OMS and repository target. This command is used to change the monitoring Agent for the target and/or the connection string used to monitor this target. The parameter descriptions are as below:</p> <ul style="list-style-type: none"> • <code>-agent <new agent></code>: Specifies a new destination agent for the emrep target • <code>-conn_desc [<jdbc connect descriptor>]</code>: Updates Connect Descriptor with the specified value. If the value is not specified, it is taken from the stored value in <code>emoms.properties</code>. • <code>-ignore_timeskew</code>: Ignores time skew on Agents.
<pre>emctl config repos [- sysman_pwd <sysman password>]</pre>	<p>Configures the repository database target. This command is used to change the monitoring Agent for the target and/or the monitoring properties (host name, Oracle Home and connection string used to monitor this target). The parameter descriptions are as below:</p> <ul style="list-style-type: none"> • <code>-agent <new agent></code>: Specifies a new destination agent for the repository target. • <code>-host <new host></code>: Specifies a new host name for the repository target. • <code>-oh <new oracle home></code>: Specifies a new Oracle home for the repository target. • <code>-conn_desc [<jdbc connect descriptor>]</code>: Updates Connect Descriptor with the specified value. If the value is not specified, it is taken from the stored value in <code>emoms.properties</code>. • <code>-ignore_timeskew</code>: Ignores time skew on Agents.

Table 7-7 (Cont.) EMCTL HA Configuration Commands

EMCTL Commands	Description
emctl enroll oms [-as_host <host>] -as_port <port> -as_pws <admin password> -nm_pwd <nodemanager password>	<p>Enrolls the OMS on to the specified Administration Server host. This command is used in the process of recovering an OMS in a multi-OMS environment. The parameter descriptions are as below:</p> <ul style="list-style-type: none"> -as_port <port>: Specifies the Administration Server secure port. -as_pwd <admin password>: Specifies the Administration Server password. -nm_pwd <nodemanager password>: Specifies the node manager password.

EMCTL Resync Commands

[Table 7-8](#) lists the EMCTL resync commands.

Table 7-8 EMCTL Resync Commands

EMCTL Commands	Description
emctl resync repos (-full -agentlist "agent names") [-name "resync name"] [-sysman_pwd "sysman password"]	<p>Submits a repository re-synchronization operation. When the -full option is specified, all agents are instructed to upload the latest state to the repository.</p> <p>The -agent parameter indicates the list of agents to re-synchronize with.</p> <p>Note: To use this command shut down the OMSes first and then submit the resync repos command. You can then start the OMSes to start the resync jobs.</p>
emctl abortresync repos (-full -agentlist "agent names") -name "resync name" [-sysman_pwd "sysman password"]	<p>Aborts the currently running repository re-synchronization operation. The -full option stops the complete repository re-synchronization, and the -agentlist option stops the re-synchronization of the list of agents.</p>
emctl statusresync repos -name "resync name"	Lists the status of the given repository re-synchronization operation.

EMCTL Connector Command

The EMCTL command to add and register a custom template on Enterprise Manager is:

```
emctl register_template connector [-t <template.xml>] [-repos_pwd <repos password>] [-cname <connectorName>] [-iname <internalName>] [-tname <templateName>] [-ttype <templateType>] [-d <description>]
```

The parameter descriptions are as below:

- t: Indicates the full path of the template.
- repos_pwd: Indicates the Enterprise Manager root (SYSMAN) password.
- cname: Indicates the connector name.
- iname: Indicates the internal name of the template.

- `-tname`: Indicates the displayed template name.
- `-ttype`: Indicates the template type. The different template types are:
 - `<templateType> 1`: inbound transformation
 - `<templateType> 2`: outbound transformation
 - `<templateType> 3`: xml based outbound transformation
- `-d`: Indicates the description.

EMCTL Patch Repository Commands

[Table 7-9](#) lists the EMCTL patch repository commands.

Table 7-9 EMCTL Patch Repository Commands

EMCTL Commands	Description
<code>emctl applypatch repos [-patchHome <patch home directory> -pluginHome <plugin home directory>]</code>	Loads the .sql files in the patch to the repository. This command has to be run from the patch directory and the path to the location where the patch is unzipped has to be specified.
<code>emctl rollbackpatch repos [-patchHome <patch home directory> -pluginHome <plugin home directory>]</code>	Recalls the .sql files from the repository to the patch directory location that is specified.

EMCTL Commands for Windows NT

The `emctl create service` command creates a service for the OMS on Windows. Use this command to manage the Windows service for the OMS on a failover host in a Cold Failover Cluster setup. This command is applicable only on Windows NT. The syntax of the command is:

```
emctl create service [-oms_svc_name <oms_service_name> -user <username>] [-passwd <password>]
```

The parameter descriptions are as below:

- `-oms_svc_name <servicename>`: Indicates the name of the OMS service to be created. If a name is not specified, the system uses the service names in the EM properties file.
- `-user <username>`: Indicates the OS user name to register the service with. If the user name is not specified, the system registers it as LocalSystem.
- `-passwd <password>`: OS password for the OS user specified.

The `emctl delete service` command deletes the service for the OMS on Windows. This command is applicable only on Windows NT. The command syntax is as below, where, `-oms_svc_name <servicename>` indicates the name of OMS service to be deleted.

```
emctl delete service [-oms_svc_name <oms_service_name>]
```

EMCTL Partool Commands

The `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 Enterprise Manager

The different flavors of the `emctl partool` command are listed below:

- `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 7-10](#) lists the EMCTL partool command options.

Table 7-10 EMCTL Partool Command Options

EMCTL Command Option	Description
<code><deploy view export></code>	Deploys, displays, or exports the <code>par</code> files.
<code>repPasswd <repPasswd></code>	Indicates the repository password.
<code>force</code>	Forces the <code>swlib</code> entities to be created or uploaded again. If they are already present, it creates a new revision.
<code>check</code>	Checks if the software library is configured.
<code>file <file></code>	Indicates the <code>par</code> file.
<code>verbose</code>	Indicates the verbose mode.
<code>help</code>	Displays the help message.
<code>displayName <displayName></code>	Indicates the <code>par</code> file name.
<code>parDir <dir></code>	Indicates the directory where the <code>par</code> files are located.
<code>metadataOnly</code>	Filters for metadata-only exports.
<code>guid <guid></code>	Indicates the procedure <code>guid</code> to export. To export multiple procedures provide the <code>guids</code> separated by comma (,).
<code>parFile <file></code>	Indicates the path of the <code>par</code> file.
<code>description <description></code>	Indicates the <code>par</code> file description.
<code>ssPasswd <secretStorePassword></code>	This parameter is optional. This parameter creates an Oracle Wallet with the specified password to store the value of the secret property in the exported software library entity. The user must use the same password while importing the <code>par</code> file in to a new repository.

Note

For more information on `emctl partool` command see the topic *Using emctl partool Utility* in the *Oracle Enterprise Manager Lifecycle Management Administrator's Guide*.

EMCTL Plug-in Commands

The EMCTL plug-in command is used to resume a previous plug-in upgrade session that had failed. If the previous failure had occurred in a schema manager session, then the execution will be resumed from failed PL/SQL block. The command syntax is:

```
emctl resume_plugin_upgrade
```

EMCTL Command to Sync with OPSS Policy Store

The EMCTL command to sync roles and users between the EM repository and the OPSS policy store is:

```
emctl sync_opss_policy_store [-force]
```

Note

If `-force` parameter is specified, it removes the OPSS application roles and role memberships that are not present in the EM.

Troubleshooting Oracle Management Service Startup Errors

Following are the log files you can check if the Oracle Management Service (OMS) fails to start:

Oracle Management Service Fails to Start

Check the logs located as indicated in [Table 7-11](#). The `INSTANCE_HOME` mentioned in the table is the OMS instance home and `n` is the index of the OMS server.

Table 7-11 OMS Log Files Location

OMS Log File	Log File Location
EMCTL log file	<code>\$INSTANCE_HOME/sysman/log/emctl.log</code> file
Managed Server log files	<code>\$INSTANCE_HOME/user_projects/domains/<DOMAIN_NAME>/servers/EMGC_OMS<n>/logs/EMGC_OMS<n>.log</code> <code>\$INSTANCE_HOME/user_projects/domains/<DOMAIN_NAME>/servers/EMGC_OMS<n>/logs/EMGC_OMS<n>.out</code>

Table 7-11 (Cont.) OMS Log Files Location

OMS Log File	Log File Location
OMS log files	\$INSTANCE_HOME/sysman/log/emoms_pbs.log
	\$INSTANCE_HOME/sysman/log/emoms_pbs.trc
	\$INSTANCE_HOME/sysman/log/emoms.trc
	\$INSTANCE_HOME/sysman/log/emoms.log
	\$INSTANCE_HOME/sysman/log/emoms_monitoring.trc
	\$INSTANCE_HOME/sysman/log/emoms_monitoring.log
	\$INSTANCE_HOME/sysman/log/emoms_login.trc
	\$INSTANCE_HOME/sysman/log/emoms_login.log
Node Manager log files	\$INSTANCE_HOME/NodeManager/emnodemanager/nodemanager.log

WebTier Service Fails to Start

Check logs under <WebTier Instance Home>/diagnostics folder in case WebTier start fails.

Troubleshooting Management Agent Startup Errors

If the agent fails to start, see the `emctl.log` and `emagent.nohup` log files for details. The log files are saved in the `$AGENT_INSTANCE_HOME/sysman/logs` directory. Following are common issues and troubleshooting suggestions:

- [Management Agent starts up but is not ready](#)
- [Management Agent fails to start due to time zone mismatch between agent and OMS](#)
- [Management Agent fails to start due to possible port conflict](#)
- [Management Agent fails to start due to failure of securing or unsecuring](#)

Management Agent starts up but is not ready

The Management Agent goes through the following process when it starts up:

1. Starting up (the Management Agent has just received the request to start up and is going to start the initialization sequence)
2. Initializing (the Management Agent is iterating over each of its components and is initializing them)
3. Ready (All components have been initialized and the Management Agent is ready to accept requests)

The command to start the Management Agent (`emctl start agent`) has a default timeout of 120 seconds. At the end of that timeout, it will return control to the caller and will indicate what the last state of the Management Agent was when it returns control. Depending on the number of targets being monitored by the Management Agent, step 2 listed above could take a long time and it is possible that when the command exits, the state of the agent is "Initializing" and the command reports that the "agent is running but is not ready".

You can increase the timeout by setting an environment variable "EMAGENT_TIME_FOR_START_STOP". The value should indicate the number of seconds to wait before returning control to the caller.

Management Agent fails to start due to time zone mismatch between agent and OMS

The Management Agent uses the time zone set in `emd.properties` file. During the install process of the Management Agent, the agent and the host target are registered with the OMS along with the time zone. If the Management Agent's time zone is modified at any point after the installation, the OMS will signal the Management Agent to shut down as soon as it detects this mismatch.

To reset the Management Agent's time zone, run the following command:

```
emctl resetTZ agent
```

For more information about setting the time zone for the agent, see the description of the `emctl resetTZ agent` command in the [Table 7-3](#).

Management Agent fails to start due to possible port conflict

If the Management Agent cannot start and EMCTL reports that there is a possible port conflict, check the Management Agent's port (based on `emd.properties:EMD_URL`) and see if there is another application, such as another agent, running on the machine that is already bound to the port.

To resolve this issue, stop the application currently bound to the Management Agent's port.

Management Agent fails to start due to failure of securing or unsecuring

Securing or unsecuring of the Management Agent can fail if the password to secure the agent against the OMS is incorrect or if the OMS is locked or down. You can find the reason for the failure in the `<agent state directory>/sysman/log/secure.log` file.

Using emctl.log File to Troubleshoot

The `emctl.log` file is a file that captures the results of all EMCTL commands you run. For Management Agent, the log file resides in the `$AGENT_INSTANCE_HOME/sysman/log` directory of the Management Agent, and for OMS, the log file resides in the `$OMS_INSTANCE_HOME/em/EMGC_OMS<n>/sysman/log/` directory. The file is updated every time you run an EMCTL command. If your EMCTL command fails for some reason, access this log file to diagnose the issue.

For example, run the following command from the Oracle home directory of the Management Agent to check its status:

For Unix:

```
<agent_instance_home>/bin/emctl status agent
```

For Windows:

```
<agent_instance_home>\bin\emctl status agent
```

After running the command, navigate to the log directory to view the following information in the `emctl.log` file:

```
13809 :: 2024-12-03 07:54:26,158::Initializing the agent command locking system
13809 :: 2024-12-03 07:54:26,185::AgentLifeCycle.pm: Processing status agent
```

```
13809 :: 2024-12-03 07:54:26,185::AgentStatus.pm:Processing status agent
13809 :: 2024-12-03 07:54:28,608::AgentStatus.pm:emdctl status returned 3
13809 :: 2024-12-03 07:54:28,611::Cleaning up agent command lock
13809 :: 2024-12-03 07:54:28,611::AgentCommandLock:closed file handle of emctl lockfile
```

Here, the first column, that is, 1114306, is the PID that was used to check the status. The second column shows the date and time when the command was run. The third column mentions the Perl script that was run for the command. The last column describes the result of the command, where it shows the progress made by the command and the exit code returned for the command. In this case, the exit code is 3, which means that the Management Agent is up and running.

Similarly, for the OMS, you can run the following command from the Oracle home directory of the Management Service to check its status:

For Unix:

```
<OMS_HOME>/bin/emctl status oms
```

For Windows:

```
<OMS_HOME>\bin\emctl status oms
```

Example 7-1 Sample Log Content for OMS

```
2024-12-02 20:27:58,830 [main] INFO wls.OMSController - Executing emctl command : status
2024-12-02 20:28:05,023 [main] INFO commands.BaseCommand - Oracle Management Server is Up
2024-12-02 20:28:05,179 [main] INFO commands.BaseCommand - statusOMS message printed via
new method for zdt apps.
2024-12-02 20:28:05,179 [main] INFO commands.BaseCommand - statusOMS finished with
result: 0
```

In another example, run the following command from the Oracle home directory of the Management Agent to upload data:

For Unix:

```
<Agent_Instance_Home>/bin/emctl upload agent
```

For Windows:

```
<Agent_Instance_Home>\bin\emctl upload agent
```

After running the command, navigate to the log directory to view the following information in the emctl.log file:

```
14882 :: 2024-12-03 08:01:24,988::AgentLifeCycle.pm: Processing upload agent
14882 :: 2024-12-03 08:01:24,988::AgentStatus.pm:Processing upload agent
14882 :: 2024-12-03 08:01:26,801::AgentStatus.pm:emdctl status agent returned 3
14882 :: 2024-12-03 08:01:28,796::AgentStatus.pm:/u01/em/agt24/agent_24.1.0.0.0/bin/
emdctl upload agent returned 0
```

Here, the entries are similar to the entries in the first example, but the exit code returned is 6, which means the upload operation is failing for some reason.

The exit codes returned depend on the emctl command executed. In general, exit code of zero means success and any exit code other than zero means failure. For details about the cause of failure, view the error message.

8

Locating and Configuring Enterprise Manager Log Files

When you install the Oracle Management Agent (Management Agent) or the Oracle Management Service (OMS), Enterprise Manager automatically configures the system to save certain informational, warning, and error information to a set of log files.

Log files can help you troubleshoot potential problems with an Enterprise Manager installation. They provide detailed information about the actions performed by Enterprise Manager and whether or not any warnings or errors occurred.

This chapter not only helps you locate and review the contents of Enterprise Manager log files, but also includes instructions for configuring the log files to provide more detailed information to help in troubleshooting or to provide less detailed information to save disk space.

This chapter contains the following sections:

- [Managing Log Files](#)
- [Managing Saved Searches](#)
- [Locating Management Agent Log and Trace Files](#)
- [Locating and Configuring Oracle Management Service Log and Trace Files](#)
- [Monitoring Log Files](#)
- [Configuring Log Archive Locations](#)

Managing Log Files

Many Enterprise Manager components generate log files containing messages that record errors, notifications, warnings, and traces.

[Table 8-1](#) describes the columns in the Log Message table. For any given component, the optional column may not be populated in the message.

Table 8-1 Message Columns

Column Name	Description
Time	The date and time when the message was generated. This reflects the local time zone.
Message Type	The type of message. Possible values are: Incident Error Warning, Notification, and Trace. In addition, the value Unknown may be used when the type is not known.
Message ID	The ID that uniquely identifies the message within the component. The ID consists of a prefix that represents the component, followed by a dash, then a 5-digit number. For example: OHS-51009
Message	The text of the error message.

Table 8-1 (Cont.) Message Columns

Column Name	Description
Target (Expanded)	Expanded target name.
Target	Target name
Target Type	Target type
Execution Context	<p>The Execution Context ID (ECID), which is a global unique identifier of the execution of a particular request in which the originating component participates. You can use the ECID to correlate error messages from different components.</p> <p>The Relationship ID, which distinguishes the work done in one thread on one process, from work done by any other threads on this and other processes, on behalf of the same request.</p>
Component	The component that originated the message.
Module	The identifier of the module that originated the message.
Incident ID	The identifier of the incident to which this message corresponds.
Instance	The name of the Oracle instance to which the component that originated the message belongs.
Message Group	The name of the group to which this message belongs.
Message Level	The message level, represented by an integer value that qualifies the message type. Possible values are from 1 (highest severity) through 32 (lowest severity).
Hosting Client	The identifier for the client or security group to which this message relates.
Organization	The organization ID for the originating component. The ID is <code>oracle</code> for all Oracle components.
Host	The name of the host where the message originated.
Host IP Address	The network address of the host where the message originated.
User	The name of the user whose execution context generated the message.
Process ID	The ID for the process or execution unit that generated the message.
Thread ID	The ID of the thread that generated the message.
Upstream Component	The component that the originating component is working with on the client (upstream) side.
Downstream Component	The component that the originating component is working with on the server (downstream) side.
Detail Location	A URL linking to additional information regarding the message.
Supplemental Detail	Supplemental information about the event, including more detailed information than the message text.
Archive	Values are Yes or No. If the checkbox is checked, the message is collected from the archive location. Otherwise, the message is collected from the live system.
Target Log Files	Link to the log files page for this target.
Log File	Log file that this message contains.

Using Log Viewer, you can do the following:

- [Viewing Log Files and Their Messages](#)
- [Searching Log Files](#)

- [Downloading Log Files](#)

Viewing Log Files and Their Messages

You can use Enterprise Manager to view messages across log files.

In particular, when you navigate in the context of a farm or domain, then the logs that you can view and search are filtered to just those associated with that farm or domain. When you navigate to Logs by way of the Enterprise menu, you can pick and choose exactly what targets you want to view and search logs against. You could also, for example pick multiple WebLogic Server targets that span across domains/farm.

For example, to view the log files and their messages:

1. From the **Enterprise** menu, select **Monitoring**, select **Logs**, then select the target from the popup target selector.

or

The Logs menu is available at the individual target label and at the parent target level. For example, for WebLogic server and for other j2ee components, the logs menu can be accessed by choosing **Logs** from the **Targets** menu. The same is applicable for parent targets like domain and farm targets.

2. In the context of a farm or domain, expand **Selected Targets** and in the row for a particular component or application, click the **Target Log Files** icon.

When you are in the context of the Enterprise menu, add targets to the Target table and click the **Target Log Files** icon.

The Log Files page is displayed. On this page, you can see a list of log files related to the target.

3. Select a file and click **View Log File**.

The View Log File page is displayed. On this page, you can view the list of messages and download the log file from this page.

4. To view the details of a message, select the message.

By default, the messages are sorted by time, in ascending order. You can sort the messages by the any of the columns, such as Message Type, by clicking the column name. The Message Type is sorted by importance from highest to lowest and uses the order of Incident Error, Error, Warning, Notification, and then Trace.

5. When you are in context of one domain or one farm and looking at logs, the related messages are confined to that one domain or one farm. For example, to view messages that are related by time or ECID, click **View Related Messages** and select **by Time** or **by ECID (Execution Context ID)**.

The Related Messages page is displayed.

When trying to view log messages, you may see the following error:

Logging Configuration is missing or invalid for the targets (). Also, make sure that these targets are up and EM User has the CONFIGURE_TARGET privilege on the corresponding domains.

To ascertain which method to use to fix the problem, choose one of these three alternatives:

- The domain's Administration Server is down. To resolve the problem, start the Administration Server and try viewing log messages again.
- The Managed Server for which you are trying to view log messages is down. To resolve the problem, start the Managed Server and try viewing log messages again.

- The Enterprise Manager administrator who is trying to access log messages does not have the necessary target privileges to do so. In order to view log messages, the administrator must have been granted the target privilege "Configure target" for the corresponding WebLogic Domain target. Talk to your Oracle Enterprise Manager site administrator or super administrator regarding whether or not you have this privilege.

Restricting Access to the View Log Messages Menu Item and Functionality

You can restrict which administrators in Oracle Enterprise Manager have access to the View Log Messages menu item and its corresponding functionality. You can grant a target privilege labeled "Ability to view Fusion Middleware Logs" to administrators and/or roles. This target privilege is applicable to all Oracle Fusion Applications related and Oracle Fusion Middleware related target types. This target privilege is automatically included as part of the following other target privileges: Operator Fusion Middleware, Operator, and Full. Consequently, you can grant an administrator one of the following privileges in order for him/her to be able to view log messages for Oracle Fusion Applications related and Oracle Fusion Middleware related log files:

- Ability to view Fusion Middleware Logs target privilege
- Operator Fusion Middleware target privilege
- Operator target privilege
- Full target privilege

To grant the ability to an administrator to view the Fusion Middleware Logs target privilege, follow these steps:

1. Log in to the Enterprise Manager console as a super administrator.
2. From the **Setup** menu, choose **Security**, then **Administrators**.
3. Select the appropriate administrator and click **Edit**.
4. Click **Next** twice to arrive on the Target Privileges page of the wizard.
5. Scroll down the page and click **Add** in the Target Privileges section of the page.
6. From the **Search and Add: Targets** popup dialog, select the appropriate targets for which the administrator should have access to view logs. Click **Select**.
7. From the Target Privileges section of the Target Privileges page of the wizard, select the targets to which you want to grant the "Ability to view Fusion Middleware Logs" target privilege and select **Grant to Selected**. Notice that the default target privilege automatically given for this target is View.
8. Select the **Ability to view Fusion Middleware Logs** target privilege and click **Continue**. Notice that the "Ability to view Fusion Middleware Logs" target privilege is also included as part of other target privileges (for example, Operator target privilege). So, depending on the responsibilities of the administrator, you may want to grant the Operator target privilege to the administrator.
9. Notice on the Target Privileges page of the wizard the appearance of the new privilege. Click **Review** and then **Finish** to conclude the operation.

Registering Additional Log Files

You may find that you want to add custom log files for WebLogic Server such that those log files and messages appear in the Enterprise Manager Log Viewer. While Enterprise Manager does not support adding custom log files via the Log Viewer user interface, there is a way to do it outside of Enterprise Manager.

Normally the ODL LogQueryMBean automatically discovers the Weblogic server logs and any ODL log file defined in the logging.xml file associated with the Weblogic server. However, you can register additional log files with the ODL LogQueryMBean, so that these files can be viewed and/or downloaded from the Enterprise Manager Log Viewer.

When registering a new log file there are two options you can use:

- You can register a log file with an associated LogReader that can be used to parse the contents of the file. In this case the contents of the file can be viewed and searched from the main Log Messages page.
- You can register the path to the log file, but do not provide a LogReader to parse the contents of the file. In this case the contents of the file cannot be viewed and searched from the main Log Messages page, but you can view the raw contents of the file or download its contents from the Target Log Files page.

To register one or more additional log files you can create a file under directory:

DOMAIN_HOME/config/fmwconfig/servers/SERVER_NAME/diagnostics-registration

The file must have a .xml suffix and it should have contents similar to the following:

```
<?xml version='1.0' encoding='UTF-8'?>
<logs xmlns='http://www.oracle.com/ias/EMComponent/ojdl'>
  <log path="/home/oracle/mylogs/my-odl-diagnostic.log">
    <logreader class="oracle.core.ojdl.reader.ODLLogReaderFactory">
    </logreader>
  </log>
</logs>
```

In this case the file is an ODL file and it is being registered with a LogReader. In addition to the ODL LogReader, there are a few existing log readers that can be used to read other formats.

You can also register a log without a log reader as seen here:

```
<?xml version='1.0' encoding='UTF-8'?>
<logs xmlns='http://www.oracle.com/ias/EMComponent/ojdl'>
  <log path="/home/oracle/mylogs/my-other-diagnostic.log"/>
</logs>
```

You may use variables or a wildcard in the log path. The wildcard is denoted by "%*%", while a variable has the form of "%NAME%". Multiple occurrences of the same variable in the path must have the exact same value. If a variable appears only once, it will behave like a wildcard.

All log files registered in this way are associated with the server target in Enterprise Manager.

Searching Log Files

You can search for diagnostic messages using the Log Messages page. By default, this page shows a summary of the logged issues for the last 10 minutes.

You can modify the search criteria to identify messages of relevance. You can view the search results in different modes, allowing ease of navigation through large amounts of data.

The following sections describe how to search log files:

- [Searching Log Files: Basic Searches](#)
- [Searching Log Files: Advanced Searches](#)

Searching Log Files: Basic Searches

You can search for all of the messages for all of the entities in a domain, an Oracle WebLogic Server, a component, or an application.

For example, to search for messages for a domain:

1. From the **Enterprise** menu, select **Monitoring**, select **Logs**, then select the target from the popup target selector.

or

From the **Targets** menu, select **Middleware**, click a farm. From the **Farm** menu, select **Logs**, then select **View Log Messages**.

The Log Messages page displays a Search section and a table that shows a summary of the messages for the last hour.

2. In the Search Mode section, you can choose to search for only **Live Logs**, only **Archive Logs**, or **Both**.
3. In the Date Range section, you can select either:
 - **Most Recent:** If you select this option, select a time, such as 3 hours. The default is 10 minutes.
 - **Time Interval:** If you select this option, select the calendar icon for **Start Date**. Select a date and time. Then, select the calendar icon for **End Date**. Select a date and time.
4. In the Message Types section, select one or more of the message types.
5. You can specify more search criteria, for example, by providing text in the Message text field, so you can search on explicit words or patterns across log files. You can specify more search criteria, as described in [Searching Log Files: Advanced Searches](#).
6. Click **Search**.
7. To help identify messages of relevance, in the table, for **Show**, select one of the following modes:
 - **Messages** - You can select an operator, such as **contains** and then enter a value to be matched.

To see the details of a particular message, click the message. The details are displayed below the table of messages.

To view related messages, select a message, then click **View Related Messages** and select **by Time** or **by ECID (Execution Context ID)**.
 - **Application ID** - Groups messages related to a particular application.
 - **ECID + Relationship ID** - Groups messages by Execution Context (ECID) and Relationship ID (RID) which enables you to use log file entries to correlate messages from one application or across application server components. By searching related messages using the message correlation information, you can examine multiple messages and identify the component that first generated the problem.
 - **Host** - Groups messages associated with a particular host.
 - **Host IP Address** - Groups messages associated with a particular host IP address.
 - **Incident ID**
 - **Message Type** - Groups messages for each target based on the message type. It displays the total number of messages available for each message type, for example,

ERROR, INCIDENT ERROR, WARNING, NOTIFICATION, TRACE, and UNKNOWN for every target.

- **Message ID** - Groups messages based on the combination of Message ID, Message Type, Target, Message Level, Component, Module, and Organization.
- **Module** - Groups the classes / modules that originated the message.
- **Target**
- **Thread ID** - Groups messages by Thread ID
- **User** - Groups all messages for a particular user. For example, all the messages for user Jones will be listed before the messages for user Smith.

Searching Log Files: Advanced Searches

You can refine your search criteria using the following controls in the Log Messages page:

- **Message:** You can select an operator, such as **contains** and then enter a value to be matched.
- **Add Fields:** Click this to specify additional criteria, such as Host, which lets you narrow the search to particular hosts. Then click **Add**.

For each field you add, select an operator, such as **contains** and then enter a value to be matched.

- **Selected Targets:** Expand this to see the targets that are participating in the search. To add targets, click **Add** and provide information in the dialog box. To remove targets, select the target and click **Remove**.
- **Search Archived Logs:** Enable this check box to access the log viewer. These are the archive log file locations for multiple targets you configured on the Configure Archive Locations page.

Note

The Search Archived Logs check box is not applicable to standalone Oracle HTTP Servers.

Downloading Log Files

You can download the log messages to a file. You can download either the matching messages from a search or the messages in a particular log file.

To download the matching messages from a search to a file:

1. From the **Enterprise** menu, select **Monitoring**, then select **Logs**.

or

From the **Targets** menu, select **Middleware**, then select a domain. From the **Farm** menu, select **Logs**, then select **View Log Messages**.

The Log Messages page is displayed.

2. Search for particular types of messages as described in [Searching Log Files: Basic Searches](#).
3. Select a file type by clicking **Export Messages to File** and select one of the following:

- **As Oracle Diagnostic Log Text (.txt)**
- **As Oracle Diagnostic Log XML (.xml)**
- **As Comma-Separated List (.csv)**

An Opening dialog box is displayed.

4. Select either **Open With** or **Save to Disk**. Click **OK**.

To export specific types of messages or messages with a particular Message ID to a file:

1. From the **Enterprise** menu, select **Monitoring**, then select **Logs**.

or

From the **Targets** menu, select **Middleware**, then select a domain. From the **Farm** menu, select **Logs**, then select **View Log Messages**.

The Log Messages page is displayed.

2. Search for particular types of messages as described in [Searching Log Files: Basic Searches](#).
3. For **Show**, select **Group by Message Type** or **Group by Message ID**.
4. To download the messages into a file, if you selected Group by Message Type, select the link in one of the columns that lists the number of messages, such as the Errors column. If you selected Group by Message ID, select one of the links in the Occurrences column.

The Messages by Message Type page or Message by Message ID is displayed.

5. Select a file type by clicking the arrow near **Export Messages to File**.

You can select one of the following:

- **As Oracle Diagnostic Log Text (.txt)**
- **As Oracle Diagnostic Log XML (.xml)**
- **As Comma-Separated List (.csv)**

An Opening dialog box is displayed.

6. Select either **Open With** or **Save to Disk**. Click **OK**.

To download the log files for a specific component:

1. From the **Enterprise** menu, select **Monitoring**, then select **Logs**.

or

From the **Targets** menu, select **Middleware**, click a domain. From the **Farm** menu, select **Logs**, then select **View Log Messages**.

The Log Messages page is displayed.

2. Expand the Selected Targets section because it is hidden by default. Click **Target Log Files**.

The Log Files page is displayed.

Select one of the possibly many Target Log Files icons. Select the icon that is associated with the target type log files you want to view.

3. Select a log file and click **Download**.
4. An Opening dialog box is displayed.
5. Select either **Open With** or **Save to Disk**. Click **OK**.

Managing Saved Searches

The following sections provide information on creating, retrieving, and managing saved searches:

- [Saving Searches](#)
- [Retrieving Saved Searches](#)
- [Managing Saved Searches](#)

Saving Searches

Saved searches save administrators time by not having to redefine the same search again in the future. Saved searches help you in diagnosing problems faster because you are only a few clicks away from accessing a saved search as opposed to redefining the search again and again.

Note: Saved searches are per administrator. Therefore when the administrator logs out of the console, the search is stored and is available the next time the administrator logs in. In other words, saved searches that one administrator defines are not accessible by another administrator.

Once you have specified search criteria as described in [Searching Log Files](#), you save it by clicking **Save Search** located at the top-right of the page. The name of the search is automatically created by concatenating fields used in the search, for example, Log Messages - Saved Search: "error", Last 1 hours, Incident Error,Error,Unknown.

Note: You can change the default name using the Manage Saved Search popup. This allows you to accept the default name and change it later.

Retrieving Saved Searches

To retrieve a saved search, follow these steps:

1. From the **Enterprise** menu, select **Monitoring**, select **Logs.**, then select the target from the popup target selector.

or

From the **Targets** menu, select **Middleware**, click a farm. From the **Farm** menu, select **Logs**, then select **View Log Messages**.

or

Access the saved search from the **Favorites** menu.

The Log Messages page appears.

2. On the Logs page, click **Saved Searches** located at the top-right of the page.
3. Choose a search.

The search results populate the Search region.

Managing Saved Searches

To manage a saved search, follow these steps:

1. From the **Enterprise** menu, select **Monitoring**, select **Logs**, then select the target from the popup target selector.

or

From the **Targets** menu, select **Middleware**, click a farm. From the **Farm** menu, select **Logs**, then select **View Log Messages**. You can manage the saved searches pertaining to the target context only.

or

Access the saved search from the **Favorites** menu and select **Manage Favorites**. You can manage all the log-saved searches which you have created irrespective of the context. You can see all the saved searches.

The Log Messages page appears.

2. On the Logs page, click **Saved Searches** located at the top-right of the page.
3. On the list, click **Manage Saved Searches**.

The Manage Favorites pop-up appears. You can:

- Change the name of the search.

When you select a row from the table, the name of search appears in the Name field at the bottom of the screen. You can edit the name of the search and click **OK** or you can click **Cancel**.

Note: When you click **OK**, you will only be changing the name of the search, not the saved search criteria. Once the search criteria is changed, the Save Searches button is enabled.

- Edit the search criteria.

Click the link of the saved search. The Log Viewer screen appears in the context of the saved search. Make the changes and click **Save**.

- Delete a search

Choose a search and click **Remove Selected**.

Locating Management Agent Log and Trace Files

The following sections provide information on the log and trace files for the Oracle Management Agent:

- [About the Management Agent Log and Trace Files](#)
- [Locating the Management Agent Log and Trace Files](#)

About the Management Agent Log and Trace Files

Oracle Management Agent log and trace files store important information that support personnel can later use to troubleshoot problems. The agent main log is located in `$EMSTATE/sysman/log`. The log is segmented by default to 11 segments, 5MB each. The segments are named `gcagent.log` and `gcagent.log.#` where # is a number in the range of 1-10. These settings are controlled by properties in `emd.properties` as explained in the following sections. The latest segment is always `gcagent.log` and the oldest is the `gcagent.log.X` where X is the highest number.

The Management Agent uses the following log files:

- Oracle Management Agent metadata log file (`gcagent.log`)

This log file contains trace, debug, information, error, or warning messages from the agent.

- Oracle Management Agent fetchlet trace file (`gcagent_sdk.trc`)

This log file contains logging information about fetchlets and receivelets.

- Oracle Management Agent errors log file (`gcagent_errors.log`)

This error log file contains information about errors. The errors in this file are duplicate of the errors in `gcagent.log`.

- Oracle Management Agent metadata log file (`gcagent_mdu.log`)

This log tracks the metadata updates to the agent.

- Enterprise Manager Control log file (`emctl.log`)

The information is saved to `emctl.log` file, when you run the Enterprise Manager Control commands. For more information about `emctl.log` file, see chapter *Starting and Stopping Enterprise Manager Components*.

Note

All the agent logs mentioned above (existing in `$EMSTATE/sysman/log`) are transient. Agent logs are segmented and have a limited overall size and hence need not be deleted or managed.

Structure of Agent Log Files

The log contain individual log messages with the following format:

```
YYYY-MM-DD HH:MM:SS,### [<tid>:<thread code or code:name>] <level> -<the message>
```

Where:

- `YYYY-MM-DD HH:MM:SS,###` is a timestamp (in 24 hours format and `###` is the fraction in msec).
- `<tid>` is the thread id (as a decimal number)
- `<thread name or code>` is the thread full name or an abbreviated hexadecimal code (see the following example).
- `<level>` is the logging level that can be one of (in ascending order of importance): `DEBUG`, `INFO`, `WARN`, `ERROR`, `FATAL`.
- `<the message>` is the free text message that is being logged. The message can contain new lines and spawn multiple lines.

For example:

```
2011-06-07 15:00:00,016 [1:3305B9:main] DEBUG - ADR_BASE='/ade/example_user/oracle/example/agentStateDir'
2011-06-07 15:00:01,883 [1:3305B9] INFO - Agent is starting up
```

Locating the Management Agent Log and Trace Files

The log and trace files for the Management Agent are written in the agent runtime directory. You can find the runtime directory by using this command:

```
$ emctl getemhome
```

The log and trace files will be located at `<EMHOME>/sysman/log`.

Setting Oracle Management Agent Log Levels

Every log message is logged using a specific log level. The log levels are ordered in priority order: DEBUG, INFO, WARN, ERROR, and FATAL. The log setting determines the minimum level that will be included in the log. For example, if the log level is set to INFO (the default), only log messages of level INFO and above (INFO, WARN, ERROR and FATAL) are going to be included in the log.

The logging configuration syntax uses the concept of handlers (appenders in log4j terms) and loggers. A handler defines a single output file and how the file is to be managed (maximum file size, number of segments, and so on). Note that there is a default logging prefix `oracle.sysman` that is used for all handlers that does not specify any logging prefix. The logging properties uses the `Logger.` prefix for agent (log4j) logging configuration and `ODLLogger.` prefix for the ODL (which is based on `java.util.logger.*`) logging configuration. Beside the prefix, both systems share the same syntax. The configuration full syntax (without a `Logger` or `ODLLogger` prefix) is the following:

Table 8-2

Property Name	Description	Mandatory	Default Value
<code>directory=<directory></code>	Defines the logging system (log4j or ODL) logging directory. Specifying a directory for one system does not affect the other system (setting <code>Logger.</code> <code>directory</code> will only affect the <code>Logger.</code> configuration but not <code>ODLLogger.</code>)	No	<code>\$EMSTATE/sysman/log</code>
<code><handler>.filename=<filename></code>	The filename to use for the handler. If the filename is relative it will be relative to the logging directory (see <code>directory</code> property above). An absolute file name will be used as is.	Yes	
<code><handler>.level=<level></code>	The default logging level for the handler. Possible levels are: DEBUG, INFO, WARN, ERROR, FATAL	Yes	
<code><handler>.totalSize=<size></code>	The total size in MB for all the handler file segments.	No	No limit
<code><handler>.segment.count=<count></code>	The number of segments to use for the handler.	No	1
<code><handler>.logger=<logger names></code>	A comma delimited list of logger names that will use this handler.	No	When not specified, the default logger is used.
<code>level.<logger name>=<level></code>	Set a specific logging level to the logger and all its descendants. Possible levels are: DEBUG, INFO, WARN, ERROR, FATAL	No	
<code>additivity.<logger name>=<true or false></code>	If set to false, only handlers that are configured for the specific logger name will be used. Otherwise, handlers that are configured for the logger parent name will also be used.	No	true

An example of the syntax is as follows:

```
# logging properties
Logger.log.filename=gcagent.log
Logger.log.level=INFO
Logger.log.totalSize=100
Logger.log.segment.count=20

ODLLogger.wsm.level=ERROR
ODLLogger.wsm.totalSize=5
ODLLogger.wsm.segment.count=5
ODLLogger.wsm.filename=gcagent_wsm.log
```

The above log configuration sets up a handler (log) that creates a gcagent.log file (in the default logging directory) with a default logging level of INFO, total size of 100MB, uses up to 20 segments, and is configured to be used by the default logger (oracle.sysman).

Modifying the Default Logging Level

To enable DEBUG level logging for the Management Agent, set the log handler level to DEBUG (see below). And then reload the agent.

```
Logger.log.level=DEBUG
```

Alternatively, use `emctl setproperty agent` command as follows:

```
$ emctl setproperty agent -name "Logger.log.level" -value DEBUG
```

or

```
$ emctl setproperty agent -name "Logger.log.level" -value "DEBUG"
```

Setting gcagent.log

The gcagent.log is the agent main log that contain log entries from all the agent core code. The following is gcagent.log configuration:

```
Logger.log.filename=gcagent.log
Logger.log.level=DEBUG
Logger.log.totalSize=100
Logger.log.segment.count=20
```

Setting gcagent_error.log

The gcagent_errors.log is a subset of the gcagent.log and contains log messages of ERROR and FATAL levels. The logging configuration for gcagent_errors.log is specified in `emd.properties`. Following are the settings for gcagent_errors.log:

```
Logger.err.filename=gcagent_errors.log
Logger.err.level=ERROR
Logger.err.totalSize=100
Logger.err.segment.count=5
```

Setting the Log Level for Individual Classes and Packages

The logging level for individual class and/or packages can also be set. The following are examples that are currently configured by default:

```
# Set the class loaders to level INFO
Logger.level.oracle.sysman.gcagent.metadata.impl.ChainedClassLoader=INFO
Logger.level.oracle.sysman.gcagent.metadata.impl.ReverseDelegationClassLoader=INFO
```

```
Logger.level.oracle.sysman.gcagent.metadata.impl.PluginLibraryClassLoader=INFO
Logger.level.oracle.sysman.gcagent.metadata.impl.PluginClassLoader=INFO
```

The above configuration changed the default level of logging for the four classes to be INFO. When the default level of logging is INFO it does not make any difference but if the default log level is set to DEBUG (when debugging the code) it will prevent those four classes from logging at DEBUG level (as they are normally too verbose).

The reverse is also true, for example if the following configuration is added (not set by default):

```
Logger.level.oracle.sysman.gcagent.metadata.impl.collection=DEBUG
```

It will cause all classes in the oracle.sysman.gcagent.metadata.impl.collection package to log at DEBUG level even if the default log level is INFO.

Setting gcagent_mdu.log

A set of entries are created in the gcagent_mdu.log file for each client command that modifies target instances, target instance collections, or blackouts. Entries are as follows:

```
2011-08-18 22:56:40,467 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] - SAVE
TARGET(S)
<Target IDENTIFIER="TARGET_GUID=6A3A159D0BB320C50B7926E0671A1A98" STATUS="MONITORED"
TIMEZONE_REGION="" ON_HOST="" DISPLAY_NAME="EM Management Beacon" NAME="EM Management
Beacon" TYPE="oracle_beacon"/>
<Target IDENTIFIER="TARGET_GUID=51F9BBC6F5B833058F4278B51E496000" STATUS="MONITORED"
TIMEZONE_REGION="" ON_HOST="" DISPLAY_NAME="mytestBeacon" NAME="mytestBeacon"
TYPE="oracle_beacon"><Property VALUE="****" NAME="proxyHost"/><Property VALUE="****"
NAME="proxyPort"/><Property VALUE="****" NAME="dontProxyFor"/></Target>
<Target IDENTIFIER="TARGET_GUID=7C4336B536C9F241DBCAC4D1D082AD22" STATUS="MONITORED"
TIMEZONE_REGION="" ON_HOST="" DISPLAY_NAME="CSAcollector" NAME="CSAcollector"
TYPE="oracle_csa_collector"><Property VALUE="****" NAME="recvFileDir"/></Target>
<Target IDENTIFIER="TARGET_GUID=207B57A3FE300C86F81FE7D409F5DD1C" STATUS="MONITORED"
TIMEZONE_REGION="" ON_HOST="" DISPLAY_NAME="Oemrep_Database" NAME="Oemrep_Database"
TYPE="oracle_database"><Property VALUE="****" NAME="MachineName"/><Property VALUE="****"
NAME="Port"/><Property VALUE="****" NAME="SID"/><Property VALUE="****" NAME="OracleHome"/>
<Property ENCRYPTED="FALSE" VALUE="****" NAME="UserName"/><Property ENCRYPTED="FALSE"
VALUE="****" NAME="Role"/><Property ENCRYPTED="FALSE" VALUE="****" NAME="password"/></
Target>
<Target IDENTIFIER="TARGET_GUID=0C48C5AE0FAFB42ED91F897FF398FC84" STATUS="MONITORED"
TIMEZONE_REGION="" ON_HOST="" DISPLAY_NAME="Management Services and Repository"
NAME="Management Services and Repository" TYPE="oracle_emrep"><Property VALUE="****"
NAME="ConnectDescriptor"/><Property ENCRYPTED="FALSE" VALUE="****" NAME="UserName"/>
<Property ENCRYPTED="FALSE" VALUE="****" NAME="password"/><AssocTargetInstance
ASSOC_TARGET_TYPE="oracle_oms"
ASSOC_TARGET_NAME="linuxserver07.myco.com:41034_Management_Service"
ASSOCIATION_NAME="app_composite_contains"/><AssocTargetInstance
ASSOC_TARGET_TYPE="oracle_oms"
ASSOC_TARGET_NAME="linuxserver07.myco.com:41034_Management_Service"
ASSOCIATION_NAME="internal_contains"/><CompositeMembership><Member ASSOCIATION=""
NAME="linuxserver07.myco.com:41034_Management_Service_CONSOLE" TYPE="oracle_oms_console"/>
<Member ASSOCIATION="" NAME="linuxserver07.myco.com:41034_Management_Service_PBS"
TYPE="oracle_oms_pbs"/><Member ASSOCIATION=""
NAME="linuxserver07.myco.com:41034_Management_Service" TYPE="oracle_oms"/></
CompositeMembership></Target>
<Target IDENTIFIER="TARGET_GUID=DF64B4A7C0F2EEBA7894EA3AD4CAF61E" STATUS="MONITORED"
TIMEZONE_REGION="" ON_HOST=""
DISPLAY_NAME="linuxserver07.myco.com:41034_Management_Service"
NAME="linuxserver07.myco.com:41034_Management_Service" TYPE="oracle_oms"><Property
VALUE="****" NAME="InstanceHome"/><Property VALUE="****" NAME="OracleHome"/>
<AssocTargetInstance ASSOC_TARGET_TYPE="oracle_oms_console"
ASSOC_TARGET_NAME="linuxserver07.myco.com:41034_Management_Service_CONSOLE"
```

```

ASSOCIATION_NAME="app_composite_contains"/><AssocTargetInstance
ASSOC_TARGET_TYPE="oracle_oms_pbs"
ASSOC_TARGET_NAME="linuxserver07.myco.com:41034_Management_Service_PBS"
ASSOCIATION_NAME="app_composite_contains"/><AssocTargetInstance
ASSOC_TARGET_TYPE="oracle_oms_console"
ASSOC_TARGET_NAME="linuxserver07.myco.com:41034_Management_Service_CONSOLE"
ASSOCIATION_NAME="internal_contains"/><AssocTargetInstance
ASSOC_TARGET_TYPE="oracle_oms_pbs"
ASSOC_TARGET_NAME="linuxserver07.myco.com:41034_Management_Service_PBS"
ASSOCIATION_NAME="internal_contains"/><CompositeMembership><MemberOf ASSOCIATION=""
NAME="Management Services and Repository" TYPE="oracle_emrep"/><Member ASSOCIATION=""
NAME="linuxserver07.myco.com:41034_Management_Service_CONSOLE" TYPE="oracle_oms_console"/
><Member ASSOCIATION="" NAME="linuxserver07.myco.com:41034_Management_Service_PBS"
TYPE="oracle_oms_pbs"/></CompositeMembership></Target>
<Target IDENTIFIER="TARGET_GUID=4D290260F13596502EFD8F3E22752404" STATUS="MONITORED"
TIMEZONE_REGION="" ON_HOST=""
DISPLAY_NAME="linuxserver07.myco.com:41034_Management_Service_CONSOLE"
NAME="linuxserver07.myco.com:41034_Management_Service_CONSOLE"
TYPE="oracle_oms_console"><Property VALUE="***" NAME="InstanceHome"/><Property
VALUE="***" NAME="OracleHome"/><CompositeMembership><MemberOf ASSOCIATION=""
NAME="Management Services and Repository" TYPE="oracle_emrep"/><MemberOf ASSOCIATION=""
NAME="linuxserver07.myco.com:41034_Management_Service" TYPE="oracle_oms"/></
CompositeMembership></Target>
<Target IDENTIFIER="TARGET_GUID=D0A23AE06A9E678221B075A216364541" STATUS="MONITORED"
TIMEZONE_REGION="" ON_HOST=""
DISPLAY_NAME="linuxserver07.myco.com:41034_Management_Service_PBS"
NAME="linuxserver07.myco.com:41034_Management_Service_PBS"
TYPE="oracle_oms_pbs"><Property VALUE="***" NAME="InstanceHome"/><Property VALUE="***"
NAME="OracleHome"/><CompositeMembership><MemberOf ASSOCIATION="" NAME="Management
Services and Repository" TYPE="oracle_emrep"/><MemberOf ASSOCIATION=""
NAME="linuxserver07.myco.com:41034_Management_Service" TYPE="oracle_oms"/></
CompositeMembership></Target>
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] - SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] - SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] - SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] - SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] - SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] - SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] - SUCCESS
2011-08-18 22:57:10,084 [HTTP Listener-34 - /emd/main/ (DispatchRequests)] - SUCCESS

```

For the batch of saved targets in the above example, the original request came in at 22:56:40 and the list of targets saved are found in the line(s) following the SAVE TARGET(S) message. In this case, there were 8 targets. The result of saving the targets is available in the next 8 lines (for the same thread) and in this case all were saved successfully by 22:57:10.

The pattern is the same for saved collection items (or collections) and blackouts.

The logging configuration for the gcagent_mdu log is specified in emd.properties but you must not modify this log. For example, these entries are logged at INFO level, which means that if you decided to save space and change this to WARN only by editing the mdu log entries in the emd.properties file, you will have effectively disabled this log.

Following are the settings for gcagent_mdu log:

```

Logger.mdu.filename=gcagent_mdu.log
Logger.mdu.level=INFO
Logger.mdu.totalSize=100
Logger.mdu.segment.count=5
Logger.mdu.logger=Mdu

```

Note

Change the filename and logger settings only if asked by Support.

Setting the TRACE Level

The following `_enableTrace` property when set to "true" will enable the TRACE logging level that shows as DEBUG messages.

```
Logger._enableTrace=true
```

The default log level for the agent log must be set to DEBUG for the tracing level to work.

Locating and Configuring Oracle Management Service Log and Trace Files

The following sections describe how to locate and configure the OMS log files:

- [About the Oracle Management Service Log and Trace Files](#)
- [Locating Oracle Management Service Log and Trace Files](#)
- [Controlling the Size and Number of Oracle Management Service Log and Trace Files](#)
- [Controlling the Contents of the Oracle Management Service Trace File](#)
- [Controlling the Oracle WebLogic Server and Oracle HTTP Server Log Files](#)

About the Oracle Management Service Log and Trace Files

OMS log and trace files store important information that Oracle Support can later use to troubleshoot problems. OMS uses the following six types of log files:

- Oracle Management Service log file (`emoms.log`)
The Management Service saves information to the log file when it performs an action (such as a starting or stopping) or when it generates an error. This is a log file for console application.
- Oracle Management Service trace file (`emoms.trc`)
OMS trace file provides an advanced method of troubleshooting that can provide support personnel with even more information about what actions the OMS was performing when a particular problem occurred. This is a trace file for Console application.
- Oracle Management Service log file (`emoms_pbs.log`)
The Management Service saves information to this log file for background modules such as the loader, job system, event system, notification system, and so on. This file contains messages logged at ERROR or WARN levels.
- Oracle Management Service trace file (`emoms_pbs.trc`)
This trace file provides additional logging for the background modules such as the loader, job system, event system, notification system, and so on when DEBUG or INFO level logging is enabled for these modules. This file can provide Support personnel with even more information about actions these modules were performing when a particular problem occurred.

- Enterprise Manager Control log file (`emctl.log`)
The information is saved to `emctl.log` file, when you run the Enterprise Manager Control commands. For more information about `emctl.log` file, see chapter *Starting and Stopping Enterprise Manager Components*.
- Enterprise Manager Control message file (`emctl.msg`)
This file is created by the HealthMonitor thread of the OMS when it restarts the OMS because of a critical error. This file is used for troubleshooting the OMS restart problem. It provides information such as the exact time when the OMS is restarted and which module has caused the crash.

Locating Oracle Management Service Log and Trace Files

The OMS Instance Base directory is `gc_inst` in the Oracle Middleware Home (middleware home). This directory stores all log and trace files related to OMS.

You can choose to change this, if you want, in the installer.

For example, if the Middleware home is `/u01/app/Oracle/Middleware/`, then the instance base location is `/u01/app/Oracle/gc_inst`. You can choose to change this, if you want, in the installer. However, you can change it for only advanced installation and not for simple installation.

Controlling the Size and Number of Oracle Management Service Log and Trace Files

OMS log and trace files increases in size over time as information is written to the files. However, the files are designed to reach a maximum size. When the files reach the predefined maximum size, the OMS renames (or rolls) the logging information to a new file name and starts a new log or trace file. This process keeps the log and trace files from growing too large.

As a result, you will often see multiple log and trace files in the OMS log directory. The following example shows one archived log file and the current log file in the `/u01/app/Oracle/gc_inst/em/EMGC_OMS1/sysman/log/` directory:

```
emoms.log  
emoms.log.1
```

To control the maximum size of the OMS log and OMS trace files, as well as the number of rollover files, run the following command, and specify details as described in [Controlling the Size and Number of Oracle Management Service Log and Trace Files](#):

```
emctl set property -name <property> -value <property value> -module logging
```

The above command will set the property for all OMSes. If you want to set it for a single OMS, then specify an extra option `-oms_name` as follows:

```
emctl set property -name <name> -value <value> -module logging -oms_name  
example.myco.com:portnumber_Management_Service
```

To set it for the current OMS, use the property `-oms_name local_oms`. To set it for any other OMS, you can provide the name of that OMS. The OMS name has to be similar to `example.myco.com:portnumber_Management_Service`.

Table 8-3 Oracle Management Service Log File Properties in the emomslogging.properties File

Property	Purpose	Example
log4j.appender.emlogAppender. MaxFileSize	When OMS log file reaches this size, then OMS copies the logging data to a new rollover file and creates a new <code>emoms.log</code> log file. The size of the log is specified in units of bytes. This property is also applicable for <code>emoms_pbs.log</code> .	log4j.appender.emlogAppender. MaxFileSize=20000000
log4j.appender.emlogAppender. MaxBackupIndex	This optional property indicates how many times OMS will rollover the log file to a new file name before deleting logging data. This property is also applicable for <code>emoms_pbs.log</code> . Note: Because the log file does not contain as much data as the trace file, it is usually not necessary to create more than one rollover file.	log4j.appender.emlogAppender. MaxBackupIndex=1
log4j.appender.emtrcAppender. MaxFileSize	When the OMS trace file reaches this size, then OMS copies the logging data to a new rollover file and creates a new <code>emoms.trc</code> log file. This property is also applicable for <code>emoms_pbs.trc</code> .	log4j.appender.emtrcAppender. MaxFileSize=5000000
log4j.appender.emtrcAppender. MaxBackupIndex	This property indicates how many times the OMS will rollover the trace file to a new file name before deleting tracing data. This property is also applicable for <code>emoms_pbs.trc</code> .	log4j.appender.emtrcAppender. MaxBackupIndex=10

Controlling the Contents of the Oracle Management Service Trace File

By default, the OMS will save all critical and warning messages to the `emoms.trc` file. However, you can adjust the amount of logging information that the OMS generates.

To change the amount of logging information generated by the OMS, run the following command:

```
emctl set property -name "log4j.rootCategory" -value "<LEVEL>", emlogAppender,  
emtrcAppender" -module logging
```

The above command will change the log level for all OMS, unless `-oms_name` option is specified.

Note

If you change the `root` logging level for the `emoms.trc` file, then a lot of messages are written to the trace file filling up the space quickly, and potentially slowing down the system. Run the following command to enable debug selectively for specific modules that need to be assessed:

```
emctl set property -name <logging module> -value DEBUG -module logging
```

Where, `<logging module>` represents the logging module from a specific subsystem.

For example, `oracle.sysman.emdrep.dbjava.loader`.

The logging level can be changed for specific modules by running the following command:

```
emctl set property -name "<CATEGORY>" -value "<LEVEL>" -module logging
```

where `LEVEL` can be `DEBUG`, `INFO`, `WARN`, or `ERROR`, and `CATEGORY` is specific to the module for which level has to be changed. To change the logging module, contact Oracle Support.

Note

The location of `emoms.trc`, `emoms.log`, `emoms_pbs.trc`, and `emoms_pbs.log` files can be changed to a different location from the default location. However, it is not advisable to do so.

Controlling the Oracle WebLogic Server and Oracle HTTP Server Log Files

Oracle Management Service is a Java EE application deployed on an Oracle WebLogic Server. Different components of the Oracle WebLogic Server generate their own log files. These files contain important information that can be used later by support personnel to troubleshoot problems.

[Table 8-4](#) lists the location of the log files for some components.

Table 8-4 Component Log File Location

Component	Location
Oracle HTTP Server (OHS)	<code><EM_INSTANCE_BASE/user_projects/domains/GCDomain/servers/<ohs_name>/logs</code> For example, <code>/u01/app/Oracle/gc_inst/user_projects/domains/GCDomain/servers/ohs1/logs</code>

Table 8-4 (Cont.) Component Log File Location

Component	Location
Oracle WebLogic	<p>The log data from WebLogic will be at:</p> <pre><EM_INSTANCE_BASE>/user_projects/domains/<domain_name>/ servers/<SERVER_NAME>/logs/<SERVER_NAME>.log</pre> <p>This log can be restricted, rotated by size, time, and other conditions from the WebLogic Console. The default settings are:</p> <ul style="list-style-type: none"> • In production mode, they are rotated at a default of 5MB. • The log level is WARNING. • The number files are restricted to 10. <p>For example,</p> <pre>/u01/app/Oracle/gc_inst/user_projects/domains/GCDomain/ servers/EMGC_OMS1/logs/EMGC_OMS1.log</pre> <p>The messages written to sysout and syserr will be available in the .out files. They cannot be rotated by size or time. They are rotated only when the server starts. They are located at:</p> <pre><EM_INSTANCE_BASE>/user_projects/domains/<domain_name>/ servers/<SERVER_NAME>/logs/<SERVER_NAME>.out</pre> <p>For example,</p> <pre>/u01/app/Oracle/gc_inst/user_projects/domains/GCDomain/ servers/EMGC_OMS1/logs/EMGC_OMS1.out</pre> <p>The node manager logs are at <INST_HOME>/NodeManager/emnodemanager and the admin server logs are at <INST_HOME>/user_projects/domains/GCDomain/servers/EMGC_ADMINSERVER/logs.</p>

By default, Enterprise Manager configures Oracle HTTP Server logs to roll over periodically to a new file, so that each file does not grow too large in size. You must also ensure that you delete the old rollover files periodically to free up the disk space. You can use an operating system scheduler, like cron on UNIX, to periodically delete the rollover files.

Note

Following are log files that you will need to maintain and manually purge:

- <gc_inst>/user_projects/domains/<domain_name>/servers/EMGC_ADMINSERVER/logs/<domain_name>.log*
- All files under <gc_inst>/user_projects/domains/GCDomain/servers/ohs1/logs/*. For example:

```
em_upload_http_access_log.*
access_log.*
em_upload_https_access_log.*
ohs1-*.log
console~OHS~1.log*
mod_wl_ohs.log*
```

For instructions on controlling the size and rotation of these log files, refer to chapter "Managing Log Files and Diagnostic Data" in *Oracle Fusion Middleware Administrator's Guide*.

For information about configuring Enterprise Manager to view Fusion Applications PL/SQL and C diagnostic log files, see chapter "Managing Oracle Fusion Applications Log Files and Diagnostic Tests" in the *Oracle Fusion Applications Administrator's Guide*.

Monitoring Log Files

You can use Log File Monitoring to monitor WebLogic Server and Application Deployment log files for specific patterns. You can set up Enterprise Manager to receive alert notifications in the context of targets when patterns are found. This allows you to be more proactive and learn of problems as an administrator before end users discover them.

Use the following topics to learn how to set up and use Log File Monitoring:

- [About Log Viewer](#)
- [Overview of WebLogic Server and Application Deployment Log File Monitoring](#)
- [Enabling Log File Monitoring](#)
- [Configuring Log File Monitoring](#)
- [Viewing Alerts from Log File Monitoring](#)

About Log Viewer

Log Viewer enables administrators to view, search, and download middleware-related log files regardless of where the files reside on disk. Complex search criteria can be specified and saved for future reference in order to help administrators quickly diagnose performance problems across multiple middleware components spanning multiple Fusion Middleware Farms and WebLogic Domains.

Note

If you want to use all features of the log viewer in Enterprise Manager, and the target domain for which you want to view log messages is SSL-enabled with a custom certificate, then log viewer features will not function properly. For most features of log viewer, the OMS makes a JMX connection to the Admin Server of that domain. The only log viewer feature that does not have the OMS make a direct JMX connection to the Admin Server is the feature used for archived log files. Instead, the agent is used for viewing archived log files.

For log viewer features to fully function in this environment, you must apply additional configuration changes. You must take the *rootca* of the custom certificate from the Admin Server target for the domain against which you want to view log messages and import it into the trust store of the OMS.

When accessing Log Viewer, default search criteria is specified for the selected target type. The administrator can then refine the search criteria based on diagnostic requirements for the particular Fusion Middleware Farm. By using the Add Fields button, you can refine the search criteria to include:

- Selecting one or more member targets of the Fusion Middleware Farm
- Specifying the date range
- Selecting the message types

- Specifying the messages to be searched
- Specifying the ECIDs to be searched
- Specifying the application name
- Specifying the user name

Once the search criteria has been defined, the administrator clicks on the search button.

The administrator modifies the search as needed and clicks the **Save Search** button on the Log Viewer.

The search criteria specified, including the targets against which the search was performed, is then saved to the Management Repository for the currently logged in administrator.

You can click on the **Saved Searches** button to retrieve and apply a previously stored Search Criteria.

You can click on the Manage Saved Searches and bring up a pop-up to edit or delete the previously Saved Search Criteria.

Overview of WebLogic Server and Application Deployment Log File Monitoring

You can use Log File Monitoring to monitor WebLogic Server and Application Deployment log files for specific patterns and thereby reduce troubleshooting time. You can set up Enterprise Manager to receive alert notifications in context of targets when patterns are found.

The Log File Monitoring metric, Log File Pattern Matched Line Count for WebLogic Server and Application Deployment target types allows you to monitor one or more log files for the occurrence of one or more search patterns. In addition, you can specify a pattern to be ignored for the log file. Periodic scanning, which occurs by default every 60 minutes, is performed against any new content added since the last scan. Lines matching the ignore pattern are ignored first, then lines matching specified match patterns result in one record being uploaded to the repository for each pattern. You can set a threshold against the number of lines matching the given pattern. File rotation will be handled within the given file.

You can also use the monitoring templates functionality, which allows an administrator to configure a metric once in a template and then apply the template to several WebLogic Server or Application Deployment targets at once, rather than having to configure each WebLogic Server log file monitoring metric individually.

If you are currently using log file monitoring via the Host target type, you should configure log file monitoring via the Fusion Middleware related target type instead so you can see alerts in context of a Fusion Middleware target.

Prerequisites to Use Log File Monitoring

Log File Monitoring requires a local Management Agent monitoring target. In other words, the host on which the log files you want to monitor reside must have a Management Agent installed and running. The operating system user who installed the Management Agent must have read access to the directories where the monitored log files reside. Log file monitoring is disabled by default. You must enable it in order to use this feature.

Enabling Log File Monitoring

Log File Monitoring is disabled by default. To enable Log File Monitoring, follow these steps:

1. From the target menu, select **Monitoring**.

2. Choose **Metric and Collection Settings**.
3. On the Metric and Collection Settings page, in the **Metrics** tab, from the **View** drop-down menu, select **All metrics**.
4. Search for **Log File Monitoring**. Against the Log File Monitoring row, click the **Disabled** link.
5. On the Edit Collection Settings: Log File Monitoring page, in the Collection Schedule section, click **Enable**. The default collection schedule is set for every 60 minutes.
6. Click **Continue**.

The Metric and Collection Settings page appears. At this point, Enterprise Manager enables Log File Monitoring but does not save the changes to the Management Repository.

7. On the Metric and Collection Settings page, click **OK**.

Enterprise Manager saves your changes to the Management Repository.

Configuring Log File Monitoring

To configure Log File Monitoring, follow these steps:

1. From the target menu, choose **Monitoring**.
2. From the Monitoring menu, select **Metric and Collection Settings**.
3. On the Metric and Collection Settings page, in the **Metrics** tab, from the **View** drop-down menu, select **All metrics**.
4. Search for **Log File Monitoring**.
5. Under the Log File Monitoring row, in the **Log File Pattern Matched Line Count** row, click the **Edit** icon on the right.
6. On the Edit Advanced Settings: Log File Pattern Matched Line Count page, in the Monitored Objects section, click **Add** to add new objects to specify settings for the log files to be monitored.

The table in the Monitored Objects section lists all log file names, match patterns, and ignore patterns set for this metric. You can specify different threshold settings for each of the columns. The Reorder button specifies which log file to scan first.

You can use a combination of wildcards and regular expressions to set your search criteria.

7. In the **Log File Name** column, enter the log file name pattern you want to search for.

When you use wildcards and/or regular expressions in the **Log File Name** column, make sure you use them only for identifying the log file names and not for identifying the location path of the log directory where the log files reside.

For example,

- If you provide `/u01/domains/EMGC_DOMAIN/servers/EMGC_OMS1/logs/%.log`, then all files that have the `.log` extension in the log directory are selected.
- If you provide `/u01/domains/EMGC_DOMAIN/servers/EMGC_OMS1/logs/%diagnostics%`, then all files that have `diagnostics` in their file names in the log directory are selected.
- If you provide `/u01/domains/%_DOMAIN%/servers/EMGC_OMS1/logs/%diagnostics%`, then it will be treated as an invalid pattern. Do not use wildcards to identify the log directory path.

8. In the **Match Pattern** column, enter the match pattern that should be considered in the log file. You can use a combination of wildcards and regular expressions. Case is ignored.
For example:
 - Set the match pattern as `FATAL`. This pattern will be true for any lines containing *fatal*.
 - Set the match pattern as `%fatal%critical%`. This pattern will be true for any lines containing *fatal* and *critical*.
9. In the **Ignore Pattern** column, enter the pattern that should be ignored in the log file. By default, `%` appears in the column; you should remove the default value if nothing should be ignored. You can use a combination of wildcards and regular expressions. Case is ignored.
 - Set the match pattern as `BEA-0023` and the ignore pattern as `warning`. This pattern searches for *BEA-0023* but ignores it if the same line contains *warning*.
 - Set the match pattern as `ADFC-1023%FAILED%`. This pattern searches for *ADFC-1023* only if it is followed by *FAILED* anywhere in the same line.
 - Set the match pattern as `BEA-%` and the ignore pattern as `BEA-1005`. This pattern searches for all patterns starting with *BEA-* but ignores *BEA-1005*.
10. In the **Warning Threshold** and **Critical Threshold** columns, set the threshold values to a number such that if the pattern occurs in the log file the specified number of times within the collection schedule, then an alert will be triggered. If the number of occurrences is specified in the advanced settings, then this factors into when alert is raised.
For example, if you set the critical threshold to 1 (if pattern found more than 1 time in log file, it is critical alert) and the number of occurrences to 2, then a critical alert is raised only when the pattern is found more than once in the log file within 2 consecutive collections.

Including the Log File Pattern Matched Line Count Metric As Part of a Monitoring Template

Once log file monitoring is enabled and configured, you can include the 'Log File Pattern Matched Line Count' metric as part of a Monitoring Template. Log file locations must be the same across targets to which the template is applied. You can apply the template to multiple WebLogic servers or Application Deployment targets at once rather than setting monitoring settings individually on a per-target basis.

If after configuring the Log File Monitoring metric the log file contains the specified patterns but the alerts are not generated in the OMS, you should do the following:

- Check whether the log file name contains a perl pattern.
- Check whether the ignore pattern contains an asterisk (*). Providing an asterisk in the ignore pattern field will also ignore all the lines which include the matched patterns.

Configuration Issues

If an error message displays indicating that logging configuration is missing or invalid for certain targets, you can try the following options.

First, the WebLogic Domain that you are accessing may not be Oracle JRF (Java Required Files) enabled. Oracle JRF consists of components not included in the Oracle WebLogic Server installation and that provide common functionality for Oracle business applications and application frameworks. To view log messages, the target must be Oracle JRF enabled. To check to see if your WebLogic Domain, for example, is Oracle JRF enabled, perform the following steps:

1. From the WebLogic Domain menu, select Target Setup submenu and then Monitoring Configuration.

2. On the Monitoring Configuration page for the domain, look for the property labeled "Can Apply JRF". The value for this property could be true or false. If the value is false, then the domain is not Oracle JRF enabled.

If the value of the "Can Apply JRF" property is true for the domain, this does not necessarily mean that all managed servers within the domain are Oracle JRF enabled. If you are unable to access log messages in the context of a specific managed server, then navigate to the relevant managed server's Monitoring Configuration page. From the Monitoring Configuration page, look for the property "Is JRF Enabled". The value for this property could be true or false. If the value is false, then the managed server is not Oracle JRF enabled.

Second, the Enterprise Manager administrator who is trying to access log messages does not have the necessary target privileges to do so. In order to view log messages, the administrator must have been granted the target privilege "Ability to view Fusion Middleware Logs" for the corresponding target. Talk to your Oracle Enterprise Manager's site administrator or super administrator regarding whether you have this privilege or not. Refer to later questions in this document for additional details on this target privilege and granting the privilege to administrators.

Viewing Alerts from Log File Monitoring

Alerts generated from the Log File Pattern Matched Line Count metric appear on the home page of the target or the Alert History page.

Triggered alerts must be manually cleared.

Configuring Log Archive Locations

You can configure the host, its credentials, and archive location information for a WebLogic domain and for all targets under the domain. You can either configure everything collectively under the target at the same time, or you can configure the targets individually.

To configure all of the targets at the same time, follow these steps:

1. From the WebLogic domain home page, select **Logs** from the WebLogic Domain menu, then select **Configure Archive Locations**.

The Configure Archive Locations page appears.

2. Select the WebLogic domain in the table, then click **Assign Host Credentials**.

An Assign Host Credentials pop-up appears.

3. Provide the requisite information and make sure that the Apply Above Host Credentials to Child Targets check box is enabled, then click **OK**.

The host name you selected now appears in the Host column of the Configure Archive Locations page, and the column also displays this host for all of the child targets.

4. Click **Assign Archive Location**.

A Remote File Browser pop-up appears.

5. Double-click a directory name to enter in the host name field, then repeat this process for each sub-directory that you want to in the field. Click **OK** when you have finished.

The directory location you selected now appears in the Archive Location column of the Configure Archive Locations page, and the column also displays this location for all of the child targets.

To configure the targets separately, follow the procedure above, except select a particular target rather than the WebLogic domain.

9

Configuring and Using Services

This chapter provides an overview of services and describes the procedures to configure and monitor services with Enterprise Manager. It contains the following sections:

- [Introduction to Services](#)
- [Creating a Service](#)
- [Monitoring a Service](#)
- [Configuring a Service](#)
- [Setting Up and Using Service Level Agreements](#)
- [Using the Services Dashboard](#)
- [Using the Test Repository](#)
- [Configuring Service Levels](#)
- [Configuring a Service Using the Command Line Interface](#)

Introduction to Services

The critical and complex nature of today's business applications has made it very important for IT organizations to monitor and manage application service levels at high standards of availability. Problems faced in an enterprise include service failures and performance degradation. Since these services form an important type of business delivery, monitoring these services and quickly correcting problems before they can impact business operations is crucial in any enterprise.

Enterprise Manager provides a comprehensive monitoring solution that helps you to effectively manage services from the overview level to the individual component level. When a service fails or performs poorly, Enterprise Manager provides diagnostics tools that help to resolve problems quickly and efficiently, significantly reducing administrative costs spent on problem identification and resolution. Finally, customized reports offer a valuable mechanism to analyze the behavior of the applications over time. Enterprise Manager monitors not only individual components in the IT infrastructure, but also the applications hosted by those components, allowing you to model and monitor business functions using a top-down approach, or from an end-user perspective. If modeled correctly, services can provide an accurate measure of the availability, performance, and usage of the function or application they are modeling.

Defining Services in Enterprise Manager

A **service** is defined as an entity that provides a useful function to its users. Some examples of services include CRM applications, online banking, and e-mail services. Some simpler forms of services are business functions that are supported by protocols such as DNS, LDAP, POP, FTP or SMTP.

Enterprise Manager allows you to define one or more services that represent the business functions or applications that run in your enterprise. You can define these services by creating one or more tests that simulate common end-user functionality. You can also define services based on system targets, or on both system and service tests.

You can create service tests to proactively monitor your services. Using these tests, you can measure the performance and availability of critical business functions, receive notifications when there is a problem, identify common issues, and diagnose causes of failures.

You can define different types of service models based on your requirement. Some of the types of service models that you can create are:

- **Generic Service:** A Generic Service is the simple service model you can create in Enterprise Manager. You can define one or more service models by associating service tests and/or associating relevant system targets that represent a critical business function.
- **Aggregate Service:** A number of services can be combined together to form an Aggregate Service. Within the context of an Aggregate Service, the individual services are referred to as **sub-services**. An Aggregate Service can also be used as a sub-service to create other Aggregate Services.

An aggregate service must contain at least one of the following: member service, system, or test. The metrics can be promoted from a member service, or a system, or a test.

You can define other service models based on your requirement.

Creating a Service

Before you create a service, you must be familiar with the concepts of service management. You must also perform the following tasks:

- Identify the locations where the Management Agents must be available to monitor the services using the appropriate service tests and protocols. For example, if your service includes HTTP based service tests or IMAP based service tests, ensure that the location of the Management Agent within your network architecture allows these tests. You must ensure that the Management Agents are installed at appropriate locations according to the network security (firewalls) and network routing guidelines.

Note that the beacon targets must already be created on the Management Agents before creating the service.

- Discover all the components for your service so that they can be listed as Enterprise Manager targets.
- Define systems on which the service is based.

You can create:

- **Generic Service - Test Based:** You can create a service that is based on a type of service test such as CalDAV, DNS, FTP, and so on.
- **Generic Service - System Based:** You can create a service that is based on a system or one or more system components.
- **Aggregate Service:** An aggregate service consists of one or more sub services which can either test based or system based generic services.

Creating a Generic Service - Test Based

To create a test based generic service, follow these steps:

1. From the **Targets** menu, select **Services**. The Services main page is displayed.
2. From the **Create** menu, select **Generic Service - Test Based**. The Create Generic Service: General page appears.

3. Enter a name for the service and select a time zone in which the service has to be monitored. The availability of the service and the SLA computation is based on the time zone you select here. Click **Next**.
4. The Create Generic Service: Service Test page appears. Select a test from the Test Type drop down list.
5. Depending on the test type you selected, enter the other parameters on this page and click **Next**. The Create Generic Service: Beacons page appears.
6. Click **Add** to add one or more beacons for monitoring the service. It is recommended that you use beacons that are strategically located in your key user communities in order for them to pro-actively test the availability of the service from those locations. If no beacons exist, you must create a new beacon. See [Deploying and Using Beacons](#) for details.

Note

- Only a single beacon should be added from a Management Agent to monitor service tests. Adding multiple beacons from the same Management Agent to a service test is not recommended.

Beacons are targets that are used to monitor service tests, primarily to measure performance of the service or business function from a different geographic location. Thus, adding multiple beacons from the same Management Agent does not add any value.

- Beacons marked as key beacons will be used to determine the availability of the service. The service is available if one or more service tests can be successfully executed from at least one key beacon.
- It is recommended that you create the beacons before you create the service.

7. Click **Next**. The Create Generic Service: Review page appears. Review the information entered so far and click Finish to create the service. The newly created service appears on the main Services page.

Creating a Generic Service - System Based

To create a system based generic service, follow these steps:

1. From the **Targets** menu, select **Services**. The Services main page is displayed.
2. From the **Create** menu, select **Generic Service - System Based**. The Create Generic Service: General page appears.
3. Enter a name for the service and select a time zone for the service. Click **Next**. The Create Generic Service: System page appears. Select a system on which the service is to be based. A system refers to the infrastructure used to host the service. A system can consist of components such as hosts, databases, and other targets.
4. Click **Next**. The Create Generic Service: Review page appears. Review the information entered so far and click Submit to create the service. The newly created service appears on the main Services page.

Creating an Aggregate Service

Aggregate services consist of one or more services, called sub services or member services. A subservice is any service created in Enterprise Manager. The availability, performance, and usage for the aggregate service depend on the availability, performance, and usage for the

individual sub services comprising the service. When creating an aggregate service, at the very least, either a system or one or more sub services must be associated. You can include both sub services and a system if required.

To create an aggregate service, follow these steps:

1. From the **Targets** menu, select **Services**. The Services main page is displayed.
2. From the **Create** menu, select **Aggregate Service**. The Create Aggregate Service: General page appears.
3. Enter a name for the aggregate service and select a time zone in which the service is to be monitored. The monitored data will be displayed in the selected time zone. Click **Next**.
4. The Create Aggregate Service: Services page appears. Click **Add** and select one or more member services (sub services) that are to be part of the aggregate service. You can add one or more test based, system based generic services, and one or more aggregate services. Click Next.
5. The Create Aggregate Service: System page appears. Select a system target on which the service is to be based. Associating a system with a service is not mandatory but is recommended. Features like Root Cause Analysis depend on key system components being correctly defined.

After you have created an aggregate service, you can add or remove its constituent sub services, modify the availability definition and add or delete performance or usage metrics.

 **Warning**

If you delete or remove a subservice from an aggregate service, the aggregate service performance, usage, and business metrics may be affected if they are based on a deleted subservice's metrics.

Monitoring a Service

After a service has been defined, you can monitor the status of the service, view the availability history, performance, enabled SLAs, topology, and so on. This section describes the following:

- Generic / Aggregate Service Home Page
- Performance Incidents Page
- SLA Dashboard
- Test Summary
- Topology

Viewing the Generic / Aggregate Service Home Page

To view the overview of the performance, availability, and usage of your service, click on a selected service in the main service pages. The Home page of the selected service appears. It contains the following regions:

- **General:** In this region, you can view the current status of the service and the availability (%) over the last 24 hours. You can also view whether the availability is based on the service test, or the system. In the case of aggregate services, availability can also be

based on the sub services. The Availability History chart shows the period of time for which the service was available, when it was down, in a blackout status, and so on.

- **Component Availability:** This region shows the availability of the service tests or system components on which the service is based. Select the **Show Only Key Tests** check box to view only the key components or tests.

Viewing the Performance / Incidents Page

On this page, you can view charts for the performance and usage metrics defined for the service and drill down to view additional metric details.

Performance metrics to help you identify how well the service test is performing for each of the remote beacons. In general, the local beacon should have a very efficient and consistent response time because it is local to the Web application host. Remote beacons provide data to reflect the response time experienced by your application end users.

Usage metrics are used to measure the user demand or workload for the service. Usage metrics are collected based on the usage of the underlying system components on which the service is hosted. You can monitor the usage of a specific component or statistically calculate the average, minimum and maximum value from a set of components.

In the Incidents and Problems region, you can view any incidents or problems associated with the service.

Viewing the SLA Dashboard

This page displays the list of enabled SLAs for this service. For each SLA, you can see the following:

- The current status of the SLA and its SLOs along with the service level value for the current SLA period.
- The History column shows the SLA status for the last seven days.
- The Violations column shows the actual, remaining, and total allowable SLA violation times for that SLO.

Viewing the Test Summary

The Test Reporting Dashboard shows the list of all the enabled tests for that particular service. Apart from the execution history of the tests over the last 24 hours, the most failed step of the test information is also displayed, both at the beacon level and at the test (aggregate) level.

The trend of the total time taken by the transaction is also displayed over the last 24 hours. Also, the breakdown of the step metrics are displayed for a particular transaction execution.

Use this page to see an overview of all the tests, by performance and issues, and to drill down to individual executions per beacon and drill down to transaction results with an execution.

How to Use This Page

By default, on arriving at this page, all the enabled tests are shown at the overall level. The most failed step information is displayed which shows the most failing step of the test across all executing beacons.

On expanding any test node in the tree-table, the beacon level execution summary is displayed showing the test execution history (last 24 hours) along with the information of the most failed step.

On clicking on the test node in the tree table, the transaction diagnostics region shows up in the lower part of page. If the parent node, that is the test (overall) node, is selected, then the diagnostics regions in the lower part show the aggregated data across all successfully executing beacons.

The left part of this region shows the transaction total time trend (last 24 hours) and has a time selector slider. The intention of this slider is to select the transaction/transaction period to see the step diagnostics region which occupies the right part of the lower region.

Viewing the Service Topology

The topology viewer provides a graphical representation of the components of your service. The topology viewer shows all dependent components and sub services, represented as icons, as well as the relationships between them, represented as links. For system components, only key components are displayed.

You can do the following:

- View the relationship between the service and its dependencies, including other services, and system key components. All determinants for your service's availability are displayed in the Enterprise Manager Topology Viewer.
- View the causes of service failure, as identified by Root Cause Analysis. Potential root causes and down targets are highlighted. Select highlighted links between components to view details on the cause of service failure. For more information, see About Root Cause Analysis. If you have installed and configured the SMARTS Network Adapter, the topology page shows the status of the network for your failed service as well. For more information on Network Manager Adapter plug-ins, refer to About the SMARTS Network Adapter.

Sub Services

Aggregate services consist of one or more services, called sub services or member services. A subservice is any generic test based on system based service. The availability, performance, and usage for the aggregate service depend on the availability, performance, and usage for the individual sub services comprising the service.

This page lists all the sub services that are part of the aggregate service. For each sub service, the status of the service, key components, incidents, and so on are displayed.

Configuring a Service

After you have created a service, you can define the service availability, associate a system with the service, define performance and usage metrics, and so on. This section describes the following:

- Availability Definition
- Root Cause Analysis Configuration
- System Association
- Service Tests and Beacons
- Test Summary
- Monitoring Settings for Tests
- Usage Metrics
- Performance Metrics

- Edit Service Level Rule

Availability Definition (Generic and Aggregate Service)

The availability of a service indicates whether the service is available to the users at any given point in time. The rules for what constitutes availability may differ from one application to another. For example, for a Customer Relationship Management (CRM) application, availability may mean that a user can successfully log onto the application and access a sales report. For an e-mail application, it may mean that the user can access the application, send and receive e-mails.

Click on the service for which you want to define the availability and navigate to the Service Home page. From the Generic Service menu, select Administration, then select Availability. The availability of a service can be based on:

- **Service Tests:** Choose this option if the availability of your service is determined by the availability of a critical functionality to your end users. Examples of critical functions include accessing e-mail, generating a sales report, performing online banking transactions, and so on. While defining a service test, choose the protocol that most closely matches the critical functionality of your business process, and beacon locations that match the locations of your user communities.

You can define one or more service tests using standard protocols and designate one or more service tests as **Key Tests**. These key tests can be executed by one or more **Key Beacons** in different user communities. You can also indicate whether the service test is a key test by enabling the Key Service Test checkbox. Only key service tests are used to compute the availability of the service. You can then select the beacons that will be used to execute the key tests and determine the availability of the service. Depending on the definition, a service is considered available if all key service tests are successful or at least one key service test is successful. See [Deploying and Using Beacons](#) for details on beacons and how to create them.

You can specify whether the service should be available when:

- All key service tests are successful (Default). This option is recommended.
- At least one key service test is successful

Note

A service test is considered available if it can be executed by at least one key beacon. If there are no key beacons, the service test will have an unknown status.

- **System:** The availability of a service can alternatively be based on the underlying system that hosts the service or selected components of the system. If availability is based on selected system components, you must select the components that are critical to running your service and designate one or more components as **Key Components**, which are used to determine the availability of the service. The service is considered available as long as at least one or all key components are up and running, depending on your availability definition.

You can specify whether the service should be available when:

- All key components are up (Default)
- At least one key component is up

You can also mark one or more components as key system components that will be used to compute the availability of the service. Key system components are used to determine

the possible root cause of a service failure. For more information, refer to "[Root Cause Analysis Configuration](#)".

- **Sub Service:** For an aggregate service, availability can also be based on the availability of the sub services. You can specify if availability should be determined based on the availability of all sub services or a single sub service.

Root Cause Analysis Configuration

You can use Root Cause Analysis (RCA) to filter a set of events to determine the cause of a higher level system, service, or application problem. RCA can help you to eliminate apparent performance problems that may otherwise appear to be root causes but which are only side effects or symptoms of the actual root cause of the problem, allowing you to quickly identify problem areas. You can view the RCA results on the Home page or Topology page of any service that is currently down. The Topology page gives you a graphical representation of the service, along with the system and component dependencies. Targets that have caused the service failure are highlighted in the Topology page.

Before running RCA, you can choose to:

- Configure the tool to run automatically whenever a service fails.
- Disable RCA by changing the default Analysis Mode to Manual.
- Define component tests for the service and thresholds for individual tests.

To configure Root Cause Analysis, follow these steps:

1. From the Service Home page, click **Monitoring Configuration**.
2. From the Monitoring Configuration page, click **Root Cause Analysis Configuration**.
3. If the current mode is set to Automatic, click **Set Mode Manual** to disable RCA. If you choose to perform the analysis manually, you can perform the analysis from the Service home page at anytime by choosing **Perform Analysis** if the service is down. If the current mode is set for Manual, click **Set Mode Automatic** to enable RCA when the state of the service and its components change
4. Click the link in the **Component Tests** column of the table for the key component you want to manage. You can then manage the key components for the service on the Component Tests page by adding, removing, or editing component tests. When a service is down, you can drill down to the key components to verify the underlying issue.

Note

When you disable RCA and set it back to automatic mode, RCA does not store the previous history results for you, thus providing no history for later reference.

Getting the Most From Root Cause Analysis

Root Cause Analysis (RCA) can provide you with great value by filtering through large amounts of data related to your services and identifying the most significant events that have occurred that are affecting your service's availability. If you are constructing your own services to manage in Enterprise Manager it is important that the services are defined with some thought and planning in order to get the most out of RCA.

The first item to consider in getting the most from RCA is the set of dependencies that your service has on other services or system components. Be sure to identify all of the system

components that your service utilizes in order to accomplish its task. If you omit a key component and the service fails, RCA will not be able to identify that component as a possible cause. Conversely, if you include components in the service definition that the service does not actually depend on, RCA may erroneously identify the component as a cause of service failures.

When building service dependencies, keep in mind that you can take advantage of the aggregate service concept that is supported by Enterprise Manager. This allows you to break your service into smaller sub-services, each with its own set of dependencies. RCA considers the status of a sub-service (a service that you depend on) as well the system components or service on which the sub-service depends.

The second item to consider in getting the most from RCA is the use of component tests. As you define the system components that your service depends on, consider that there may be aspects of these components that may result in your service failure without the component itself failing. Component tests allow RCA to test the status not only of the target itself but also the status of its key aspects.

The RCA system allows you to create component tests based on any metric that is available for the key component. Remember, this includes any metric extension that you have created for the component, allowing you great flexibility in how RCA tests the aspects of that component should your service fail. RCA can be configured to run in two modes. It can run automatically based on the failure of a service or can be configured to run manually. You can decide the mode based on the Expected Service Level Agreement % of the service being monitored. If the Expected Service Level Agreement % is high, you must select the automatic mode to ensure that possible errors and the root cause of the failure is easily detected.

System Association

A system is the set of infrastructure components (hosts, databases, application servers, etc.) that work together to host your applications. For example, an e-mail application can be hosted by a database, listener, application server, and the hosts on which these components reside.

After you create a service, you can specify the associations between the components in the system to logically represent the connections or interactions between them. For example, you can define an association between the database and the listener to indicate the relationship between them. These associations are displayed in the topology viewer for the system. Some data centers have systems dedicated to one application or service. Alternatively, others have systems that host multiple services. You can associate single or multiple services to a System, based on how the data center is set up.

Use this page to select the Enterprise Manager system that will be used to host this service. You can do the following:

- Add or select a system
- Change or remove a selected system

After you have selected the system, mark one or more system components as key components that are critical for running the service. These key components are used to determine service availability or identify causes of service failure.

Monitoring Settings

For each service, you can define the frequency (which determines how often the service will be triggered against your application) and the performance thresholds. When a service exceeds its performance thresholds, an alert is generated.

To define metrics and thresholds, from the **Generic Service** menu, select **Administration**, then select **Monitoring Settings for Tests**. The Metric and Policy Settings page is displayed. Click the **Monitoring Settings** link. The Monitoring Settings - Thresholds page appears.

- **View By Metric, Beacon** - In this view, you can click **Add Beacon Overrides** to override the default threshold values for one or more beacons. In this case, the default thresholds will only be used for beacons without any overrides. Any new beacons added to the service will use the default thresholds. Click **Add Metric** to add one or more metrics.
- **View By Beacon, Metric** - In this view, you can click on the **Default** icon to toggle between Edit and View modes for a specific metric. In the Edit mode, you can modify the parameters of the metric. You can also modify the parameters of the metric for a specific beacon. In the View mode, the default parameters of the metric will be used.
 - **View By Step, Metric, Beacon:** In this view, you can click **Add Beacon Overrides** to override the default threshold values for one or more beacons. In this case, the default thresholds will only be used for beacons without any overrides. Click **Add Metric** to define thresholds for one or more metrics.
 - **View By Step, Beacon, Metric:** In this view, you can click on the **Default** icon to toggle between Edit and View modes for a specific metric. In the Edit mode, you can modify the parameters of the metric for a specific beacon. In the View mode, the default parameters of the metric will be used. Incidents are generated only if the value of the Data Granularity property is set to ' Step'.

To define the default collection frequency and collection properties, click the **Collection Settings** tab on the Monitoring Settings page. You can do the following:

- Specify the default collection frequency for all the beacons. To override the collection frequency for a specific beacon, click **Add Beacon Overrides**.
- Specify the collection properties and their corresponding values for one or more beacons.

Service Tests and Beacons

You can add additional service tests and specify one or more beacons that will execute these service tests. To add a service test or modify an existing service test, click the **Service Test and Beacons** link in the **Monitoring Configuration** page. The Service Tests and Beacons page appears. You can select a test type from the drop down list and create a service test.

Defining Additional Service Tests

You can create different types of service tests based on the protocol and the location of the beacons. From the Service Tests and Beacons page, you can do the following:

- Add one or more service tests for your service. Select the Test Type and click **Add**. Some of the test types that can be defined are ATS, FTP, , DNS, SOAP and others.
- After you have created the service test, you must enable it. If your service test is not enabled, it will not be executed by any of the beacons. You can define one or more service tests as key tests. These key tests are used to monitor the availability and performance of your service. Only service tests that are enabled can be designated as key tests. To set up a service test as a key test, click the **Availability Definition** link at the bottom of the page.
- Create, add, or remove a beacon. When you identify the beacon locations, select locations on your internal network or on the Internet that are important to your e-business. These are typical locations where your end users are located. For example, if your business is hosted in Canada and you have customers in the United States, use a beacon installed on a host computer in the United States to measure the availability and performance of your applications.

- After you have created the service test, you can verify it by clicking **Verify Service Test**. The Status icon indicates the status of the service test i.e. whether it can be successfully executed by the key beacons. If there are no key beacons defined for the service, the status will be unknown even if there are other beacons executing the service test. Click **Status** to go to the Status History page.

Note

- While defining a SOAP (Simple Object Access Protocol) service test, if the WSDL URL to be accessed is outside the company's intranet, proxy settings need to be added to the `$OMS_HOME/sysman/config/emoms.properties` file.

For example, to set up `www-myproxy.myco.com` as proxy, specify the values as follows:

```
proxyHost=www-myproxy.myco.com
```

```
proxyPort=80
```

```
dontProxyFor=myco.com,mycorp.com
```

The `proxyUser`, `proxyPwd`, `proxyRealm`, and `proxyPropsEncrypted` properties are used to configure an authenticated proxy. After you have modified the proxy settings, you must restart all the OMSes for the changes to be effective.

In this chapter, we have covered the creation of the ATS test type as an example.

Deploying and Using Beacons

A beacon is a target that allows the Management Agent to remotely monitor services. A beacon can monitor one or more services at any point in time.

Note

Before you create a beacon, you must ensure that the Oracle Beacon 12.1.0.2 or higher plug-in has been deployed.

To create a beacon to run one or more service tests, follow these steps:

1. From the **Targets** menu, select **Services** to view the Services page.
2. From the **Services Features** menu, select **Beacons** and then click **Create**.
The Create Beacon page appears.
3. Enter the following details:
 - Name: Name of the beacon being created.
 - Agent: Select the Management Agent on which the beacon will be running.
 - Proxy Information: If the beacon is accessing the service through a firewall, you must specify the proxy server settings as follows:
 - Proxy Host and Port: The name of the proxy server host and through which the beacon communicates.

- Proxy Authentication Realm: The authentication realm (used for Basic and Digest authentication schemes) that is used to verify the credentials on the proxy server.
 - Proxy Authentication Username: The (fully qualified) username to be used for proxy server authentication.
 - Proxy Authentication Password: The accompanying password to be used for proxy server authentication.
 - Enable Message ID Request Header: Select the checkbox to include an additional header in HTTP requests issued when HTTP Ping service tests are executed. This allows Real User Experience Insight (RUEI) monitoring of HTTP Ping tests.
4. Click **Create** to create the beacon and return to the Beacon Home page. You can now use the beacon to monitor service tests.
 5. From the Generic Service menu, select **Administration**, then select **Service Tests and Beacons**. You will see a list of service tests that have been enabled along with a list of beacons.
 6. Select the service test to be monitored, then from the Beacons table, select the beacon that you have created. Indicate if it is a key beacon.
 7. Click **Verify Service Test** to execute the service test by the selected beacon.

Configuring the Beacons

This section lists additional beacon related configuration tasks.

- **Configuring SSL Certificates for the Beacon:** When a beacon is used to monitor a URL over Secure Sockets Layer (SSL) HTTPS URL, the beacon must be configured to recognize the Certificate Authority that has been used by the Website where that URL resides.

To use the SSL option with the Port Checker test, you may need to add additional certificates to the Management Agent's monitoring wallet. To add an additional certificate, follow these steps:

1. Obtain the certificate, which is in Base64encoded X.509 (.CER) format, in the b64SiteCertificate.txt file. (The file name may be different in your configuration.) An example of the contents of the file is given below:

```
-----BEGIN CERTIFICATE-----
MIIDBzCCAnCgAw...
..... base 64 certificate content .....
-----END CERTIFICATE-----
```

This file is stored in the Home directory of the Management Agent as <AGENT_BASE>/agent_inst/sysman/config/b64InternetCertificate.txt file.

2. Create the b64InternetCertificate.txt file in the agent core and instance directory if it does not exist.

```
<AGENT_BASE>/agent_inst/sysman/config/b64InternetCertificate.txt
<AGENT_BASE>/core/12.1.0.2.0/sysman/config/b64InternetCertificate.txt
```

3. Append the Base64encoded X.509 certificate to the end of both b64InternetCertificate.txt files. Include both the BEGIN and END CERTIFICATE lines.
4. Restart the Management Agent.

- **Configuring Dedicated Beacons:** Beacon functionality on an agent requires the use of an internal Java VM. The use of a Java VM can increase the virtual memory size of the

agent by several hundred megabytes. Because of memory constraints, it is preferable to create beacons only on agents that run on dedicated hosts. If you are running large numbers of tests (e.g., several hundred per minute) on a given beacon, you may also wish to install that beacon's agent on a dedicated host. To take full advantage of dedicated hardware, edit the agent's `$ORACLE_HOME/sysman/config/emd.properties` file. as follows:

`applicationmetadataquota`: the disk quota in bytes for each application area

- Set the property, `ThreadPoolModel=LARGE`. This allows the agent to simultaneously run many threads.
- Set the property, `useAllCPUs=TRUE`. This allows the agent to run on multiple CPUs simultaneously.
- The `applicationMetadataQuota_BEACON` property determines the total size that can be used to store ATS zip files. If you are using a ATS zip file or need to configure a large number of small ATS zip files on the beacon, you must specify a higher value for the `applicationMetadataQuota_BEACON` property.
- @ This property determines the total size that the beacon can consume to store @ ATS zip files. If the user intends to use large ATS zip files or wishes to @ configure large number of small ATS zip files on a beacon then this property @ should be appropriately increased.
- Append `-Xms512m -Xmx1024m` to the `agentJavaDefines` property. This increases the Java VM heap size to 1024 MB.
- **Configuring a Web Proxy for a Beacon:** Depending on your network configuration, the beacon may need to be configured to use a Web proxy. To configure the Web proxy for a beacon, search for the beacon in the All Targets page. Select the beacon you wish to configure and click **Configure**. Enter the properties for the Web proxy. For example, to set up `www-proxy.example.com` as the beacon's Web proxy, specify the values as the following:

```
Proxy Host: www-proxy.example.com
Proxy Port: 80
Don't use Proxy for: .example.com,.example1.com
```

Performance Metrics

Performance metrics are used to measure the performance of the service. If a service test has been defined for this service, then the response time measurements as a result of executing that service test can be used as a basis for the service's performance metrics. Alternatively, performance metrics from the underlying system components can also be used to determine the performance of the service.

Performance metrics to help you identify how well the service test is performing for each of the remote beacons. In general, the local beacon should have a very efficient and consistent response time because it is local to the Web application host. Remote beacons provide data to reflect the response time experienced by your application end users.

You can do the following:

- Add a performance metric for a service test. After selecting a metric, you can choose to:
 - Use the metric values from one beacon. Choose this option if you want the performance of the service to be based on the performance of one specific location.

- Aggregate the metric across multiple beacons. Choose this option if you want to consider the performance from different locations. If you choose this option, you need to select the appropriate aggregation function:

Table 9-1 Beacon Aggregation Functions

Function	Description
Maximum	The maximum value of the metric from data collected across all beacons will be used. Use this function if you want to measure the worst performance across all beacons.
Minimum	The minimum value of the metric from data collected across all beacons will be used. Use this function if you want to measure the best performance across all beacons.
Average	The average value of the metric will be used. Use this function if you want to measure the 'average performance' across all beacons.
Sum	The sum of the metric values will be calculated. Use this function if you want to measure the sum of all response times across each beacon.

- Add a performance metric for the underlying system components on which the service is hosted. After selecting a metric for a target, you can choose to:
 - Use the metric from a specific component. Choose this option if you want the performance of the service to be based on the performance of one specific system component. If you select this option, you can choose the Rule Based Target List.
 - Aggregate the metric across multiple components. Choose this option if you want to consider the performance from multiple components. If you choose this option, you need to select the appropriate aggregation function.

Table 9-2 System Aggregation Functions

Function	Description
Maximum	The maximum value of the metric across all components will be used as the value of this performance metric for the service.
Minimum	The minimum value of the metric across all components will be used as the value of this performance metric for the service.
Average	The average value of the metric across all components will be used.
Sum	The sum of values of metrics across all components will be calculated.

Note

When a system is deleted, performance metrics associated with the system will not be collected.

- Edit a performance metric that has been defined. For service test-based performance metrics, you can modify the beacon function that should be used to calculate the metric values. For system-based performance metrics, you can modify the target type, metric, and whether the aggregation function should be used. You can also modify the Critical and Warning thresholds for the metric.
- Delete a performance metric that has been defined.

Note

If you are defining performance metrics for an aggregate service, you can:

- Add performance metrics from a single sub service.
- Specify statistical aggregations of more than one metric.

After selecting the metrics, you can set the thresholds to be used to trigger incidents, or remove metrics that are no longer required.

Rule Based Target List

The Rule Based Target List is applicable for system based performance metrics and direct members of system. You can define a rule that matches a system component you have selected. System components that match the user-provided rule will participate in the metric evaluation process. Later if any system component is added that matches this rule, this component will also participate in the metric evaluation process. If any system component that matches the rule is removed, that component will not participate in the metric evaluation process. The rule you define can be based on:

- All (All system components)
- Contains (Any system component that contains given criteria)
- Starts With (Any system component that starts with given criteria)
- Ends With (Any system component that ends with given criteria)
- Equals (Any system component that matches with given criteria)

Static Based Target List

In this case, the dependent targets that are selected will participate in the metric evaluation and the targets that are not selected will not be included.

Usage Metrics

Usage metrics are used to measure the user demand for the service. Usage metrics are collected based on the usage of the underlying system components on which the service is hosted. You can monitor the usage of a specific component or statistically calculate the average, minimum and maximum value from a set of components. For example, if you are defining an email service, which depends on an IMAP server, then you can use the 'Total Client Connections' metric of the IMAP server to represent usage of this email service. You can define usage metrics only for services that are associated with a system. You can do the following:

- Add a usage metric. After selecting a metric for a target, you can choose to:
 - Use the metric from a specific component. Use this option if you want to monitor the usage of a specific component.
 - Aggregate the metric across multiple components. Use this option if you want to statistically calculate the usage across multiple components. If you choose this option, you need select the appropriate aggregation function.

Table 9-3 Aggregation Functions - Usage Metrics

Function	Description
Maximum	The maximum value of the metric across all components will be used as the value of this usage metric for the service.
Minimum	The minimum value of the metric across all components will be used as the value of this usage metric for the service.
Average	The average value of the metric across all components will be used.
Sum	The sum of the values of metrics across all components will be calculated.

- Edit a usage metric that has been defined.
- Delete a usage metric that has been defined.

Note that only metrics from system targets can be added as usage metrics. Metrics from tests are not indicative of usage, and therefore cannot be added as usage metrics.

Note

If you are defining usage metrics for an aggregate service, you can

- Add usage metric from a single sub service.
- Specify statistical aggregations of more than one metric.

After selecting the usage metrics, you can set the threshold to be used to trigger incidents or remove metrics that are no longer required.

Rule Based Target List

The Rule Based Target List is applicable for system based performance metrics and direct members of system. You can define a rule that matches a system component you have selected. This enables you to promote performance metrics for evaluation. System components that match the user-provided rule will participate in the metric evaluation process. Later if any system component is added that matches this rule, this component will also participate in the metric evaluation process. If any system component that matches the rule is removed, that component will not participate in the metric evaluation process. The rule you define can be based on:

- All (All system components)
- Contains (Any system component that contains given criteria)
- Starts With (Any system component that starts with given criteria)
- Ends With (Any system component that ends with given criteria)
- Equals (Any system component that matches with given criteria)

Setting Up and Using Service Level Agreements

A service level agreement (SLA) is a contract between a service provider and a customer on the expected quality of service for a specified business period. An SLA consists of one or more service level objectives (SLOs) for different business calendars and different service periods for which define the service levels to be provided. Whether an SLA is satisfied or not is based on the evaluation of the underlying SLOs. Service level indicators (SLIs) allow SLOs to be quantified and measured. An SLO can have one or more SLIs.

SLOs define the service level objectives to be provided. An SLO is a logical grouping of individual measurable Service Level Indicators (SLIs). For example, an SLO can define the percentage of time a service is available to the user, how well the service is performing in terms of response time or volume, and so on. Service Level Indicators (SLIs) are quantifiable performance and usage metrics that can be used to evaluate the quality of a service.

To create an SLA, follow these steps:

1. Log in to Enterprise Manager as a user with `EM_ADMINISTRATOR` role.
2. From the **Targets** menu, select **Services**.
3. Click on a Generic Service target on the list. The Service Home page is displayed.
4. From the **Generic Service** menu, select **Service Level Agreement**, then select **Configuration**. The Service Level Agreement Configuration page appears.
5. On this page, you will see a list of all the SLAs defined for the selected service. Select an SLA from the list to view the details in the Service Level Agreement Details table. You can create an SLA or make a copy of an existing SLA (Create Like).
6. In the Service Level Agreement region, click **Create**. The Configure Service Level Agreement page appears.

Figure 9-1 Create Service Level Agreement: Configure Service Level Agreement

Service Level Agreement

Configure Service Level Agreement | Configure Service Level Objective | Enable Service Level Agreement | Review

Create Service Level Agreement : Configure Service Level Agreement

This is the first step in creating a new Service Level Agreement (SLA). Provide data for all the required fields and click Next.

Create Service Level Agreement

Define Service Level Agreement to measure, and ensure the maintenance of service goals

* Service Level Agreement Name: SLA3

Description: Monthly SLA requiring 85% on exp

Customer:

Lifecycle Status: Definition

Time Zone: (UTC-08:00) US Pacific Time

* Service Level Agreement Period: Monthly

* Begin: 8/27/2012

Agreement Period: Expire

Service Level Agreement Evaluation Options

Blackout Condition ☐ Include blackout times (planned downtimes) in Service Level Objective evaluation

☐ Include time as met

☒ Include time as not met

Enter the following details:

- Name and description of the SLA.
- Name of the customer for whom the SLA is being created.
- The Lifecycle Status of the SLA. When an SLA is being created, it will be in the Definition Stage. For more details on the Lifecycle Status, see [Lifecycle of an SLA](#).
- Specify the SLA Period. This is the contractual time period for which the SLA is determined and/or evaluated for compliance. (ie. quarterly, monthly, weekly SLA). Click the **Select** icon and select Monthly, Weekly, or Daily. Enter the Frequency which the SLA is to be evaluated and the date from which the SLA is to be evaluated. The SLA goals are reset when the SLA is evaluated.

For example, if you specify the SLA Evaluation Period as Monthly, Frequency as 12 and the date as 09/01/24, the SLA will be evaluated on that date followed 11 consecutive evaluations in the months of October, November, and so on.

- Specify the SLA Agreement Period. This is the **From** and **To Date** for which the recurring SLA periods are in effect. If you do not specify the **To Date** here, the SLA will have an Indefinite expiry date.

- An SLO may sometimes not be evaluated due to planned downtime or blackouts that have been scheduled for a service. In the Service Level Agreement Evaluation Options region, select the **Include blackout times (planned downtimes) in Service Level Objective evaluation** checkbox and specify whether the blackout times are to be included in the SLO evaluation. You can choose to:

- Include time as met
- Include time as not met
- Exclude the blackout time during the overall computation of the SLO.

For example, if the blackout or planned downtime for the week is 1 day, then the weekly availability is $(7-1) / (7-1)$ days which is still 100% availability.

By default, the **Include blackout times (planned downtimes) in Service Level Objective evaluation** option is not selected.

- Click **Next**. In the Service Level Objectives page, define one or more SLOs that are to be part of the SLA. You can select the Evaluation Condition for the SLA which can be:

- All Service Level Objectives must be met.
- At least one Service Level Objective must be met.

An SLA must have at least one SLO. More than one SLO can be active at any given time. You can either specify if all SLOs or at least one SLO should be met.

- Click **Create** to define a new SLO. See [Creating a Service Level Objective](#) for details.

- You can add more SLOs or edit the SLO you have defined. Click **Next**. In the Enable Service Level Agreement page, you can specify when the SLA is to be enabled. You can select:

- Do Not Enable: If the SLA is not enabled, it will be in the Definition state and can be modified if required.
- Enable Now: If the SLA is enabled, it cannot be modified as it will be in an Active state.
- Enable Later: The SLA can be enabled later on a specified date.

- Click **Next**, review details of the SLA, and click **Submit**. The SLA will be enabled on the specified date and you will return to the Service Level Agreement Configuration page.

Actionable Item Rules for SLAs

The table below shows a list of actions that can be performed on an SLA based on its status.

Status of SLA	Create Like	Edit	Enable	Disable	Delete
Definition	Yes	Yes	Yes	No	Yes
Scheduled	Yes	Yes	No	Yes	No
Active	Yes	No	No	Yes	No
Retired	Yes	No	No	No	Yes

- An SLA in a **Scheduled** or **Active** state cannot be directly deleted. You have to disable the SLA before you can delete it.
- When you edit an SLA in a **Scheduled** state, the status of the SLA changes to **Definition**.

Creating a Service Level Objective

A Service Level Objective measures the service level of one or more indicators for a specified measurement window. Service Level Objectives (SLOs) define the service levels to be provided. You can specify if the SLA is considered to be satisfied if:

- All Service Level Objectives are met.
- At least one Service Level Objective is met.

To create an SLO, follow these steps:

1. Click **Create** in the Configure Service Level Objective page. The Create Service Level Objective page appears.

Figure 9-2 Create Service Level Objective

Configure Service Level Objective : Create Service Level Objective

This is the first step in defining a new SLO. This is a sub-wizard of the overall create Service Level Agreement wizard. On completion or cancel of this, the flow will return to the Create Service Level Agreement wizard.

Service Level Objective Conditions

A Service Level Objective measures the service level of one or more indicators for a specified measurement window. Service Level Objectives (SLOs) define the service levels to be provided. Specify SLOs for an SLA. The Service Level Agreement defined is logical grouping (AND / OR) of all the SLOs.

* Name: SLO1 Type: Performance

Service Level Percentage

* Expected Service Level (%): 85.000 ☒ Generate service level warning when below warning alert level
 * Warning Alert Level (%): 90.000

Measurement Window

Select the time periods for the SLO to be tracked and measured. One or more calendars can be chosen and configured as either includes and excludes. Including a calendar will stretch the measurement window and excluding a calendar will constrict the measurement window.

View	Add	Remove	Business Calendar	Description	Include/Exclude
			All Day Monitoring	Always on over the entire week.	<input checked="" type="radio"/> Include <input type="radio"/> Exclude

2. Enter the following details:

- Name of the SLO being defined.
- Type of SLO: The SLO can be based on Availability or Performance metrics.
- Expected Service Level%: This indicates the percentage of time the SLO conditions are met to ensure that the SLA is satisfied.
- Warning Alert Level%: If the SLO conditions do not meet the specified threshold, a critical alert is generated.

For example, if the Expected Service Level% is 90% and the Actual Service Level% is in the range of 90 to 99%, a Warning Alert is generated. If the Actual Service Level% is lesser than 90%, a Critical Alert is generated. This indicates that the SLA has been breached. If the Actual Service Level% is greater than 99%, it indicates that the SLA conditions have been satisfactorily met.

- Measurement Window: The time periods during which the SLO is in effect. A measurement window can have more than one time period assigned. For example, a measurement window can be configured as weekday peak hours which are Monday to Friday, from 9AM to 6PM and the weekend peak hours as 10AM to 2PM.

While creating an SLO, you can choose more than one Business Calendar for an SLO. For example, suppose you want to evaluate each SLO from 8AM to 5PM except at lunch time (12PM to 1PM). You can create two measurement windows and exclude the lunch time from being measured.

Another example of merging two measurement windows is when you want to combine weekly evaluation with calendar evaluation. If you want to evaluate an SLO every

Monday and on the 15th of every month, you can create two monitoring windows and include these conditions in both the windows.

By default, there are 3 predefined business calendars. You can also create your own calendar. See [Defining Custom SLA Business Calendars](#) for details.

3. Click **Next**. In the Create Service Level Indicators page, you can add one or more SLIs or conditions that allow the SLO to be measured.

Figure 9-3 Create Service Level Indicators

Configure Service Level Objective : Create Service Level Indicators Back Step 2 of 2 Submit Cancel

This step allows definition of one or more Service Level Indicators (SLI). A SLI definition requires selecting a service metric followed by the condition against which it will be measured.

Service Level Indicators

Service Level Indicators (SLIs) allow Service Level Objectives to be measured and quantified. A SLI Metric expression describes something that must evaluate to TRUE in order for the Indicator to be in the Green state. Example : In the case of availability , the expression might say that a target is in the UP state or in the BLACKOUT state. In the case of performance, the expression would say that a metric must be less than some critical threshold. The Service Level Indicator is considered to be violated if the rule specified below evaluates to false.

Evaluation Option ☒ All Service Level Indicators must be met.
☐ At least one Service Level Indicator must be met.

View + Add - Remove

Metric Name	Comparison Operator	Value
Nursery Size (MB)	>=	20.0

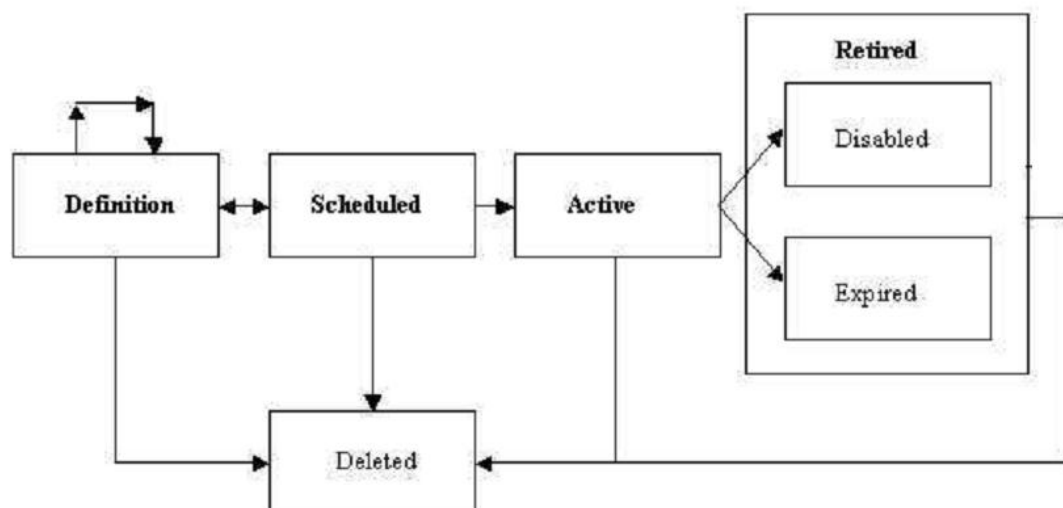
For example, if you are adding a performance SLI, you can specify that the Page Load Time should be less than or equal to 3 seconds. If this condition is not met, the SLI is considered to be violated. Specify the Evaluation Condition for the SLI:

- All Service Level Indicators must be met.
 - At least one Service Level Indicator must be met.
4. Click **Add** to add one or more metrics and specify the value and the evaluation condition. Click **Submit** to return to the Configure Service Level Objective page.

Lifecycle of an SLA

The following diagram shows the lifecycle of an SLA.

Figure 9-4 SLA Lifecycle



The SLA lifecycle consists of the following phases:

- **Definition:** This is the stage where the SLA is created and the SLOs are defined. You can configure or edit the SLA definition till the SLA is activated.
- **Scheduled:** This stage represents the period before the SLA is scheduled to go into effect at a future date.
- **Active:** This is the stage where the start date of a scheduled SLA is reached, or when the SLA is manually enabled.
- **Retired:** This is the stage when the SLA reaches the Expiry Date or the SLA is manually disabled.
- **Disabled:** An SLA can be manually disabled before it reaches the Expiry Date. Once an SLA is disabled, it cannot be reactivated. You must use the Create Like option to create a similar SLA and enable it.
- **Expired:** This is the stage where the SLA has reached the Expiry Date and is no longer active.
- **Deleted:** An SLA can be deleted if it is the Definition or Retired stage. An SLA that is an Active or Scheduled stage cannot be deleted.

Viewing the Status of SLAs for a Service

You can view the status of all SLAs for a service. To view the current status of the SLAs for a service, follow these steps:

1. From the **Targets** menu, select **Services**.
2. Click on a Generic Service target on the list. The Service Home page is displayed.
3. From the **Generic Service** menu, select **Service Level Agreement**, then select **Current Status**. The Service Level Agreement Current Status page appears.
4. This page shows a list of all the active SLAs that have been defined for this service. For each SLA, the SLA Status, SLA Evaluation Period, and the Service Level Objectives are displayed.
5. Select an SLA to view detailed information in the SLA. The following details are displayed:
 - **Tracking Status:** This is the instant status of the SLI. For an Availability SLO, it is the status of the target. For a Performance SLO, it is the value of the Performance or Usage metric at a specific point in time.
 - **Service Level (%) :** The percentage of time (from the beginning of the current evaluation period till the current date) the SLO conditions are met or the Tracking Status is **true**. If the Actual Service Level % is lesser than the Expected Service Level %, or the SLO conditions are met, the Service Level % graph is green.
 - **Type:** This is the type of SLOs that have been defined for the SLA. This can be based on Availability or Performance metrics. An Availability SLO is based on the Response Metric [Service Target Availability]. It is specified in terms of the amount or percentage of time when the availability objective should be met. A Performance SLO gauges how well a service is performing. It includes measurements of speed and/or volume such as throughput or workload (ie. response times, transactions/hour). A Performance SLO can either be specified in terms of a set of SLIs, SLO conditions, and the amount or percentage of time when the objective should be met.
 - **SLO Violation:** The violation allowances for each SLA evaluation period.
 - **Total:** The duration of the Evaluation Period * (Expected Service Level).

- **Actual:** The time when the SLO is not met during the Evaluation Period.
- **Remaining:** The time when the SLO could not be met without breaching the SLA. If the SLO is always met during the Evaluation Period, it indicates that there are no used allowances and the value in the Actual field will be 0.

Defining Custom SLA Business Calendars

Business Calendars are measurement windows that define a specific window of time in which the Service Level Objectives (SLO) are being measured. Out-of-the-box predefined business calendars are available. Apart from these, you can create custom business calendars. To create a custom business calendar, from the **Targets** menu, select **Services**. From the **Services Features** menu, select **Business Calendars**.

A list of business calendars that have been defined is displayed here. You can:

- **Create:** Click **Create** to set up a business calendar. The Add / Edit Business Calendar page is appears.
- **Create Like:** Select a calendar and click **Create Like** to make a copy of this calendar.
- **Edit:** Select a calendar, click **Edit** and make the necessary changes in the Add / Edit Business Calendar page.
- **Delete:** Select a calendar and click **Delete** to delete it. You cannot edit or delete a business calendar that is associated with one or more SLAs.
- **View Associated Service Level Agreements:** A business calendar can be used by one or more SLAs. Select a business calendar and click **View Associated Service Level Agreements** to view the SLAs that are associated with this calendar.

Using the Services Dashboard

The services dashboard provides a brief summary of all service related information in a single place. It provides a consolidated view of critical aspects of a service such as availability, performance, SLAs associated with the service, status of key system components, and so on.

Viewing the All Dashboards Page

To view the All Dashboards page, follow these steps:

1. From the **Targets** menu, select **Services**.
2. From the **Services Features** menu, select **Dashboards**.
3. The All Dashboards page appears where you can see a list of all dashboards that have been created.
4. From the All Dashboards page, you can do the following:
 - **Create Dashboard:** Enter a unique name in the Dashboard Name field and a description, and click **Create Dashboard**. The newly added dashboard appears in the table. To create a dashboard, you must have an `EM_ADMINISTRATOR` role with **Create Services Dashboard** privilege.
 - **Customize Dashboard:** Select a dashboard from the list and click **Customize** and make the changes in the Edit Services Dashboard page. The dashboard can be customized only by the user who has created it.
 - **Delete:** Select a dashboard from the list and click **Delete**. The selected dashboard is deleted. The dashboard can be deleted only by the user who has created it.

- Click on a Dashboard Name link to drill down to the Dashboard Details page.

Viewing the Dashboard Details Page

This page displays the following details:

- Service Name:** Click on the link to drill down to the Service Details page.
- Incidents:** Any incidents that have occurred.
- Performance / Usage Metric:** The name of the performance and usage metrics available for the service and the latest value of each metric is displayed. The Trend charts show the metric trend over the last 24 hours. Click on the Trend chart to see a detailed view over the trend.
- SLA:** Shows the number of enabled SLAs that are in Active, Critical or Warning state.
- Key Components:** Shows the key targets that are up or available for this service.
- System Incidents:** Any incidents that have occurred for the underlying systems of the service are displayed.

Figure 9-5 Services Dashboard

Services > All Dashboards > Dashboard (My Dashboard)

Services Dashboard

View

Service Name	Type	Status	Incidents	Performance Metric			Usage Metric			SLA
				Metric Name	Latest Value	Trend (last 24 hours)	Metric Name	Latest Value	Trend (last 24 hours)	
sys svc 1	Generic Service	↑	-	Nursery Size (MB)	-	-	Status	1		-
svc 1	Generic Service	↑	✖ 3	Perceived Time per Page (ms)	392		Not Configured			✖ 1
				HTML Time (ms)	65					
				Connect Time (ms)	212					
EM Console Service	EM Service	↑	-	Perceived Time per Page (ms)	129		Page Hits (per minute)	0		-
EM Jobs Service	EM Service	↑	-	Throughput - Job Steps/sec	0		Job Dispatcher Processing Time (% of last hour)	89.04		-
				Backlog - Jobs Steps	0					

You can filter the list of services that are listed in the dashboard. Specify a value in the Filter By field and click **Filter**. The filter will be applied on each row in all the services and the resulting list is displayed.

You can email a dashboard to one or more email addresses. Click Email and enter the email address and the subject of the dashboard. Click Send. This feature works only the http mode.

Customizing and Personalizing the Dashboard

You can customize a dashboard and make the changes available to all users. To customize a dashboard, select a row on the All Dashboards page and click **Customize**.

Note

The following privileges are required to cr

To add one or more services to the dashboard, click the Wrench icon. The Component Properties: Services Dashboard window appears. Select the type of service that you want to add to the dashboard and click **Search**. A list of services is displayed in the Available Targets table. Select one or more services that you want to add, move them to the Selected Targets table and click **Apply**. To add metrics to the respective services click on the Metrics tab and select the respective services to add metrics and click **OK**. The selected services and metrics now appear in the Services Dashboard table.

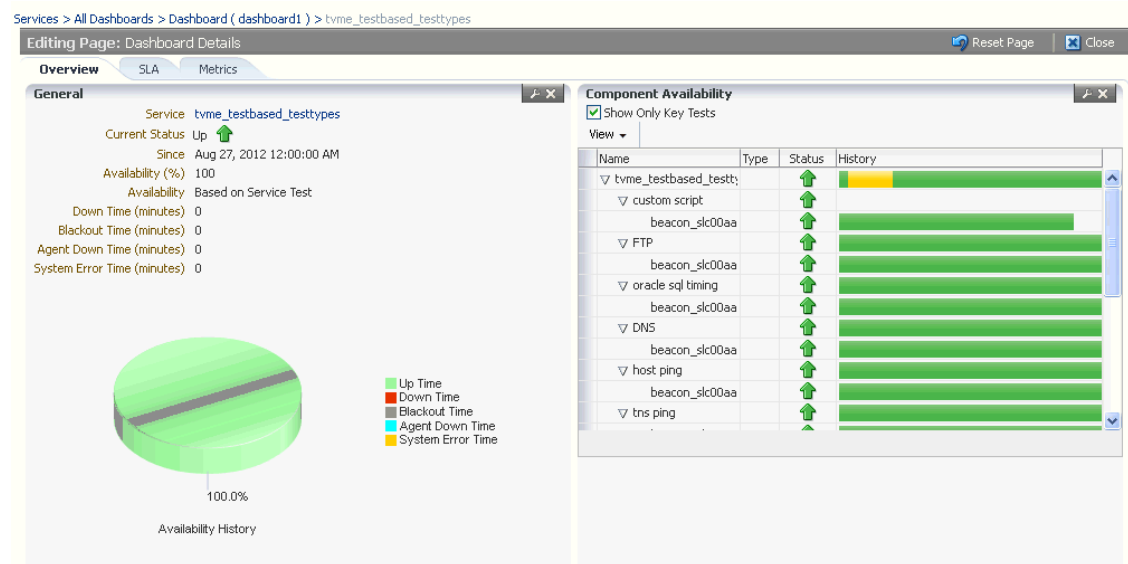
To delete a service target from the dashboard, select the row and click the Wrench icon. The Component Properties: Services Dashboard window appears. Deselect the services and metrics that are to be removed from the dashboard, click **Apply** and then click OK. To reset the changes you have made to the dashboard, click **Reset Page**. Any changes that have been made to the dashboard will be removed permanently. Click **Close** to exit the Edit mode.

You can make specific changes to a dashboard to suit your requirements. Click the **Personalize** icon and add or delete one or more services from the dashboard. The changes that you make will be visible only to you and the other users cannot see the changes.

Viewing the Dashboard Service Details Page

This page shows detailed information for the selected service.

Figure 9-6 Dashboard Details Page



It contains the following tabs:

- **Overview:** This tab provides a brief overview of the selected service. Click on the Service link to drill down to the Service Home page. It contains the following regions.
 - **General:** This region shows the name of the service, status, date from which the service is available, availability percentage, type of service (test or system based), down time, and error time. Click on the service name to drill down to the Service Home page.
 - **Component Availability:** This region shows the status of the components in the service. It shows the status of the component and the date from which the service has been Up. Select the Show Only Key Tests check box to view only the key service tests

- **SLA:** Shows a list of SLAs that have been enabled for this service. The name, status and the date from which the SLA is applicable is displayed. The SLA history over the last 7 days is also displayed.
- **Metrics:** This tab shows the performance and metrics charts that have been defined for this service. It also shows the incidents that have occurred for the service and the underlying systems on which the service is based.

Using the Test Repository

A test repository is a centralized location where you can maintain all the test scripts. To use the Test Repository, you should have pre-configured the OMS Software Library location. For more information, see [Configuring Software Library Storage Location](#).


The advantages of using a Test Repository include:

- Previously, a test could be created only in the context of a service. However, now, you have the flexibility of creating any number of test scripts outside the context of a service, and storing them in this centralized location called *Test Repository*. Uploading Test Scripts and Creating Services are now independent events. Once the test scripts are available in the repository, you can use them while creating your service.
- Previously, only the owner of the test script had the copy of the script. Now, with introduction of Test Repository, the scripts are maintained in a centralized location which allows all the users to access the scripts. At the time of creating a service, you can just import your scripts from the repository with the click of a button, thereby making the whole experience very user-friendly and quick.

Note

Currently, ATS test scripts can be stored in the central repository.

Test Repository

Page Refreshed Mar 10, 2014 9:01:00 AM UTC 

Services > Test Repository

This page shows the list of all the stored tests in the test repository. New tests can be added by clicking on the add button.

List of Stored Tests

View ▾ Add Edit Remove

Name	Type	Folder Location
New ATS test	ATS Transaction	ServiceTest/OATS/

Viewing the Test Repository

To view the test scripts uploaded to the test repository, follow these steps:

1. From the **Targets** menu, select **Services**.
2. From the **Services Features** menu, select **Test Repository**.

3. The Test Repository page appears where you can see a list of all the tests that have been created.
4. From the Test Repository page, you can do the following:
 - **Create Tests:** You can create the following types of tests:
 - **ATS Tests:** Click **Create**. In the Test Information section, select ATS Transaction in the Type drop down list and enter a unique test name and description. In the ATS Information section, click **Browse** to upload a test script from your local machine. Once you select a relevant file, the file name along with the step and module details are displayed. Click **Save** to save the script.
 - **Editing Tests:** Select the test, and click **Edit**. You can edit the following types of tests:
 - The ATS script cannot be modified within the Enterprise Manager Console. But you can download a previously uploaded script and import the zip file to ATS OpenScript. For more information on how to download and edit an ATS script, see [Editing an ATS Script](#).
 - **Removing Tests:** Select the test, and click **Delete** to delete the test script.
 - **Viewing Tests:** Click the test name to view the details of the test in the Test Details table.

Editing an ATS Script

To download the script bundle and edit them, follow these steps:

- Click **Download** and save the zip file at the prompt.
- Launch OpenScript and from select File menu select Import Script to import the zip file to ATS OpenScript.
- After you have edited the script in ATS OpenScript, select **File**, then select **Export Script** to export the new script and save the zip file.
- Log in to Enterprise Manager, and navigate to the ATS Service Test page. Click **Upload** to upload the updated script file to Enterprise Manager.

Configuring Service Levels

A service level rule is defined as an assessment criteria used to determine service quality. It allows you to specify availability and performance criteria that your service must meet during business hours as defined in your Service Level Agreement. For example, e-mail service must be 99.99% available between 8am and 8pm, Monday through Friday.

A service level rule specifies the percentage of time a service meets the performance and availability criteria as defined in the Service Level Rule. By default, a service is expected to meet the specified criteria 85% of the time during defined business hours. You may raise or lower this percentage level according to service expectations. A service level rule is based on the following:

- **Business Hours:** Time range during which the service level should be calculated as specified in your Service Level Agreement.
- **Availability:** Allows you to specify when the service should be considered available. This will only affect the service level calculations and not the actual availability state displayed in the console. You can choose a service to be considered up when it is one or more of the following states:
 - **Up:** By default the service is considered to be Up or available.

- Under Blackout: This option allows you to specify service blackout time (planned activity that renders the service as technically unavailable) as available service time.
- Unknown: This option allows you to specify time that a service is unmonitored because the Management Agent is unavailable be counted as available service time.
- **Performance Criteria:** You can optionally designate poor performance of a service as a Service Level violation. For example, if your Website is up, but it takes 10 seconds to load a single page, your service may be considered unavailable.
- **Business Criteria:** Business criteria are useful in determining in the health of the business processes for a particular service. You can optionally define business metrics that can affect the Service Level. A Service Level violation occurs when a critical alert is generated for a specified business metric.

Note

The **Business Criteria** column is displayed only if one or more key business indicators are associated with the service. Refer to the *Oracle Enterprise Manager Integration Guide*.

- **Actual Service Level:** This is calculated as percentage of time during business hours that your service meets the specified availability, performance, and business criteria.
- **Expected Service Level:** Denotes a minimum acceptable service level that your service must meet over any relevant evaluation period.

You can define only one service level rule for each service. The service level rule will be used to evaluate the **Actual Service Level** over a time period and compare it against the **Expected Service Level**.

Defining Service Level Rules

A Service Level Rule is defined as assessment criteria to measure Service quality. A Service Level Rule is based on the following:

- Time range for which the rule is applicable.
- Metrics that define the rule.
- The user expectation on these metrics values

The Expected Service Level is the expected quality for the service and is defined based on the time range and metrics of the Service Level Rule. For example, the Expected Service Level can be that the service is available 99% of the time during business hours.

When you create a service, the default service rule is applied to the service. However, you must edit the service level rule for each service to accurately define the assessment criteria that is appropriate for your service. To define a service level rule:

1. Click the **Targets** tab and **Services** subtab. The Services main page is displayed.
2. Click the service name link to go to the Service Home page.
3. In the Related Links section, click **Edit Service Level Rule**.
4. On the Edit Service Level Rule page, specify the expected service level and the actual service level and click **OK**. The expected service level specifies the percentage of time a service meets the performance, usage, availability, and business criteria defined in the Service Level Rule. The actual service level defines the baseline criteria used to define

service quality and includes business hours, availability, performance criteria, usage criteria, and business criteria.

Note

Any Super Administrator, owner of the service, or Enterprise Manager administrator with OPERATOR_TARGET target privileges can define or update the Service Level Rule.

Viewing Service Level Details

You can view service level information directly from the either of the following:

- **Enterprise Manager console** -From any Service Home page, you can click on the Actual Service Level to drill down to the Service Level Details page. This page displays what Actual Service Level is achieved by the service over the last 24 hours/ 7 days / 31 days, compared to the Expected Service Level. In addition, details on service violation and time of each violation are presented in both graphical and textual formats.
- **Information Publisher** - Information Publisher provides an out-of-box report definition called the Services Dashboard that provides a comprehensive view of any service. From the Report Definition page, click on the **Services Monitoring Dashboard** report definition to generate a comprehensive view of an existing service. By default, the availability, performance, status, usage, business, and Service Level of the service are displayed. The Information Publisher also provides service-specific report elements that allow you to create your own custom report definitions. The following report elements are available:
 - **Service Level Details:** Displays **Actual Service Level** achieved over a time-period and violations that affected it.
 - **Service Level Summary:** Displays service level violations that occurred over selected time-period for a set of services.
 - **Services Monitoring Dashboard:** Displays status, performance, usage, business, and service level information for a set of services.
 - **Services Status Summary:** Information on one or more services' current status, performance, usage, business, and component statuses.

Configuring a Service Using the Command Line Interface

Using the Command Line Interface, you can define service targets, templates and set up incidents. EMCLI is intended for use by enterprise or system administrators writing scripts (shell/batch file, perl, tcl, php, etc.) that provide workflow in the customer's business process. EMCLI can also be used by administrators interactively, and directly from an operating system console. Refer to *Enterprise Manager Command Line Interface Guide* for details.

10

Connecting to Enterprise Manager Desktop Version

You can log in to the desktop version of Enterprise Manager using a mobile device, provided your device is on the same network as Enterprise Manager. If you are remote, you may need to establish a VPN connection.

1. Connect to a WiFi or mobile network.
2. Establish a VPN connection if necessary.
3. Open your device's Web browser and specify an Enterprise Manager URL.
4. Enter login credentials to access Enterprise Manager.

With Enterprise Manager open on your iDevice, you have access to the full feature set. Consider the following as you navigate around the interface:

- Practice gestures to get a sense of how to zoom on a piece of screen real estate.
- Be patient when tapping menu selections; it does not necessarily occur instantaneously.
- Touch and hold a selection to open a context (right-click) menu. This gesture too requires some practice to develop the right sensitivity.
- Not all pages render precisely.
- Pages that have Flex/Flash effects will not render at all.

Note

If you connect to the desktop version of Enterprise Manager through a mobile Web browser, be sure to set the AutoFill Names and Passwords configuration setting to OFF. Otherwise, the login credentials can be saved to the local store, where they are susceptible to apps scanning for sensitive data.

Part II

Integrating with Oracle Cloud Infrastructure

This section contains the following chapter:

- [Integrating Enterprise Manager with OCI Services](#)
- [Generative AI Assistant](#)

Integrating Enterprise Manager with OCI Services

Enterprise Manager allows Oracle Cloud Infrastructure's (OCI) cloud services to easily utilize target-level data managed by Enterprise Manager.

Note

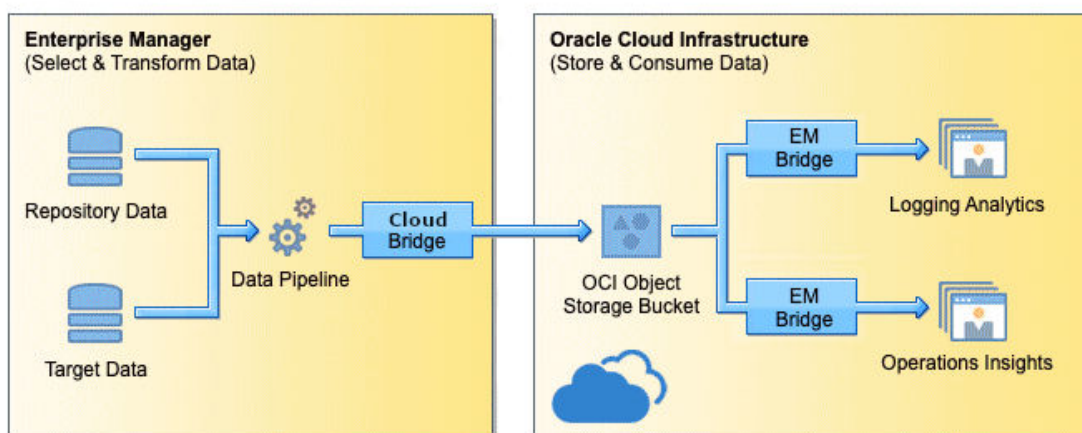
Extraction of data from Oracle Enterprise Manager Oracle Database targets into an Oracle Cloud Infrastructure service requires Oracle Diagnostics Pack on the Oracle Enterprise Manager Oracle Database targets. See Oracle Diagnostics Pack and Base Framework Feature Summary for more information.

Enterprise Manager lets you transfer data from Enterprise Manager targets and Oracle Management Repository (OMR) to OCI Object Storage, where it is easily accessed by one or more cloud-native services.

Once OCI connectivity is set up, your target data is automatically uploaded at frequent intervals to Object Storage so that OCI cloud services are always working with the most recent target data.

The following graphic illustrates how target data flows from Enterprise Manager to an OCI service once the configuration process has been completed.

Overview of using Enterprise Manager Data in OCI Services



Updating Enterprise Manager

Beginning with Enterprise Manager 13c Release 5, Update 3 (13.5.0.3), in addition to the OMS, Release Updates must also be applied to any agents monitoring targets whose data is being exported to Object Storage using the Cloud Bridge feature.

Prerequisites

Before you can set up Enterprise Manager to OCI connectivity, make sure the following prerequisites have been met.

- [Ensure an OCI Object Storage Bucket has already been created](#)
- [Set up an exclusive user for the Enterprise Manager login](#)
- [Define a Host Preferred Credentials for all target hosts including the OMS host](#)
- [Define a Global Named Credential in Enterprise Manager for OCI](#)
- [Create an Enterprise Manager group containing the targets for which you want data exported](#)
- [Set up OCI Policies to allow Enterprise Manager to push data into Object Storage](#)
- [Access from OMS Hosts and Target Hosts](#)

Note

Learn more about connecting Enterprise Manager with OCI Ops Insights by watching these videos:

- [How to connect Enterprise Manager with OCI - Step 1 OCI prerequisites](#)
- [How to connect Enterprise Manager with OCI - Step 2 Create Cloud Bridge](#)
- [How to connect Enterprise Manager with OCI - Step 3 Create an EM Bridge](#)

Ensure an OCI Object Storage Bucket has already been created

Exported target data is stored in an OCI Object Storage bucket where it can be accessed by an OCI service. Ensure that an Object Storage bucket with visibility set to private is available before setting up OCI connectivity. Make a note of you OCID, User OCID, Public Key Fingerprint, Private Key and Region. For more information, see [Required Keys and OCIDs](#) and [Where to Get the Tenancy's OCID and User's OCID](#).

Note

The OCI Object Storage Bucket cannot have any retention policy.

Set up an exclusive Enterprise Manager Super Administrator user for the Enterprise Manager login.

Oracle recommends that you set up an exclusive Enterprise Manager Super Administrator user login dedicated to exporting data from Enterprise Manager to OCI Object Storage, specifically a user name that identifies a particular Enterprise Manager instance. For example, you might define a user called *EM-austin@mycompany.com* instead of *john_doe_admin*. Creating an instance-specific user name allows for the data flowing into Object Storage to be attributed to an Enterprise Manager instance instead of an actual user.

Additionally, creating an instance-specific user name protects against security keys being invalidated if a user leaves the company.

For more information about creating users in Enterprise Manager, see [Creating Enterprise Manager User Accounts](#).

Define a Host Preferred Credentials for all target hosts including the OMS host.

To facilitate data export, you must define Host Preferred Credentials for all hosts having agents that are monitoring targets as well as the host where the OMS is installed. The user provided in the preferred host credential should be the same as the user that was used to push the agent on the host. This user should have read, write and execute privileges on the content in the agent folder. In addition, create a *Preferred Credential* for the host(s) where the primary and any additional Oracle Management Services (OMS) are installed. For more information about Host Preferred Credentials, see [Host Authentication Features](#).

Ensure that the Database Plug-in has been pushed to all OMS hosts. The Database Plug-in is usually pushed by default with an agent, so verify that it has not been removed.

Verify that the OMS host(s) and hosts that have agents monitoring the database targets that are included in the data extraction have connectivity to OCI/Object Storage.

Define a Global Named Credential in Enterprise Manager for OCI

A Named Credential allows you to create a user name/password pair that is stored in Enterprise Manager as a *named* entity, thus allowing the credential to be used without having to expose the actual password. A Named Credential can be defined on a single target, such as a single database or host. Global Named Credentials are defined as *global* in scope, which makes the credentials available on all targets of a specific type.

A Global Named Credential needs to be defined for use when exporting Enterprise Manager target data to OCI Object Storage. To create a Global Named Credential,

1. From the **Setup** menu, choose **Security** and then **Named Credentials**.
2. Click **Create**. The Create Credential page displays.
3. From the Authenticating Target Type drop-down menu, select **Oracle Cloud Infrastructure**. Property details change according to the selected target type.
4. Set Scope to **Global**.
5. Fill in the requisite properties and click **Save**.

Note

For more information about Named Credentials and their application, see [Named Credentials](#).

Private key needs to be generated from the command line via `openssl` (as shown in OCI documentation). Currently the private key generated and downloaded directly from the OCI Console does not work for this feature. For more information about OCIDs and Keys, see [Required Keys and OCIDs](#).

Create an Enterprise Manager group containing the targets for which you want data exported.

In order to export Enterprise Manager target data to OCI, the relevant targets must be members of a group. When defining a source for OCI Service Data Export, you will select a target group and not individual targets. Be sure to make note of this group name.

Note

For Ops Insights, when adding an Exadata Database Machine to a group, ensure that the `osm_cluster/osm_instance` targets are listed. If they are not listed, then you must manually add them to the group being enabled for Ops Insights.

For information about groups, see [Managing Groups](#).

Set up OCI Policies to allow Enterprise Manager to push data into Object Storage

You need to set up OCI policies to ensure that Cloud Bridge has proper access. Choose the approach that meets your business needs:

- Least Restrictive

```
Allow group <GroupOfCloudBridgeUser> to manage object-family in
compartment <BucketCompartment> where all {target.bucket.name='BucketA'}
```

- More Restrictive

```
Allow group <GroupOfCloudBridgeUser> to manage objects in compartment
<BucketCompartment where all {target.bucket.name='BucketA'}
Allow group <GroupOfCloudBridgeUser> to read buckets in compartment
```

To use Cloud Extensions with Enterprise Manager, allowing the OCI Ops Insights Cloud Extension (EM Dashboard) content to appear within the database target home page, as well as in other Ops Insights locations, the following policy is required:

```
Allow group <GroupOfCloudBridgeUser> to read opsi-family in compartment
<HighestCompartmentContainingOPSResource>
```

Note

Enter the policy statement at the highest level possible for every compartment you wish to place Ops Insights resources in.

For more details, see [Let Object Storage admins manage buckets and objects.](#)

Access from OMS Hosts and Target Hosts

The OCI Ops Insights service communicates with its own endpoints and Object Storage endpoints during the Enterprise Manager data export. These endpoints are derived from the Object Storage URL provided during the Cloud Bridge setup.

If there's a firewall or proxy server used to control access to the internet for the agents monitoring the targets, ensure that both the Object Storage URL as well as the Ops Insights URL are added to the allowlist of the firewall and proxy server to ensure seamless Enterprise Manager data export.

Examples of Object Storage URLs:

- For `us-phoenix-1` (OC1): <https://objectstorage.us-phoenix-1.oraclecloud.com>
- For `ap-chiyoda-1` (OC8): <https://objectstorage.ap-chiyoda-1.oraclecloud8.com>

Examples of Ops Insights URLs:

- For us-phoenix-1 (OC1): <https://operationsinsights.us-phoenix-1.oci.oraclecloud.com>
- For ap-chiyoda-1 (OC8): <https://operationsinsights.ap-chiyoda-1.oci.oraclecloud8.com>

Setting Up OCI Service Connectivity

Configuring OCI service connectivity requires setup of both Enterprise Manager and the OCI service. The content of this chapter focuses primarily on the Enterprise Manager setup. Links to OCI service documentation that contains service-specific Enterprise Manager integration procedures are provided in Step 2.

Note

Before you can complete these steps, ensure that the prerequisites have been met. For more information about these prerequisites, see [Prerequisites](#)

Enterprise Manager to OCI service connectivity configuration is performed in two steps:

- [Step 1: Export Enterprise Manager Data to OCI](#)
- [Step 2: Import Data from the Object Storage Bucket to the OCI Service](#)

Step 1: Export Enterprise Manager Data to OCI

To move target data from Enterprise Manager to OCI, you create a Cloud Bridge in Enterprise Manager. The Cloud Bridge defines a data connection to the OCI Object Storage bucket residing in OCI.

To create the Cloud Bridge in Enterprise Manager, do the following:

Note

Bridge creation is a one-time setup. Once created, it can be edited, updated or deleted as needed.

Log in as the newly created data exporting Super Administrator user recommended earlier and create a Cloud Bridge.

1. From the **Setup** menu, choose **Cloud Bridge**. The Cloud Bridge page displays. This page will be empty the first time you access it.
2. Click **Manage OCI Connectivity**.
OCI Bridge is selected by default.

Enter the following for the OCI Bridge:

- **OCI Credential:** The credential name you created above.
- **Base URL:** The base URL for the Storage Bucket.
Syntax: <https://objectstorage.<region>.<domain>>

Examples:

- For us-phoenix-1 (OC1): `https://objectstorage.us-phoenix-1.oraclecloud.com`
- For ap-chiyoda-1 (OC8): `https://objectstorage.ap-chiyoda-1.oraclecloud8.com`
- For me-dcc-muscat-1 (OC9): `https://objectstorage.me-dcc-muscat-1.oraclecloud9.com`

Note

If using Ops Insights, the endpoints are also derived from the above Object Storage URL for data export jobs. See below some examples of Ops Insights URLs for different regions:

- For us-phoenix-1 (OC1): `https://operationsinsights.us-phoenix-1.oci.oraclecloud.com`
- For ap-chiyoda-1 (OC8): `https://operationsinsights.ap-chiyoda-1.oci.oraclecloud8.com`
- For me-dcc-muscat-1 (OC9): `https://operationsinsights.me-dcc-muscat-1.oci.oraclecloud9.com`

If there's a firewall or proxy server used to control access to the internet for the agents monitoring the targets, ensure that both the Object Storage URL as well as the Ops Insights URL are added to the allowlist of the firewall and proxy server.

- **Bucket:** The bucket name.
- **Proxy Credentials:** (Optional) The proxy credentials to be used when connecting to the object storage while transferring the files. The proxy credentials are created from the Enterprise Manager console under **Security, Named Credentials**. Under **Target Type**, select *Cloud Bridge*. Under **Credential Properties**, enter the proxy details: host, port, username and password.

You can use an existing proxy server when using Cloud Bridge Proxy Credentials to capture the proxy details. Another option is to set up Cloud Bridge with OCI Management Gateway service if the proxy is not accessible/available where the EM instance is deployed. In this case, you need to install Management Gateway on the DMZ or Gateway server to send the data to OCI. For information about OCI Management Gateway service, see [Management Gateway](#).

Note

Starting with Enterprise Manager 13c Release 5 Update 15 (13.5.0.15), Cloud Bridge supports the specification of proxy details which are used for outbound connections to OCI. This release update (patch) needs to be applied to the OMS, central agent and all other participating agents.

- **Saved As:** A name for the bridge you are about to create.

Then, click **Create** to create the new OCI Bridge.

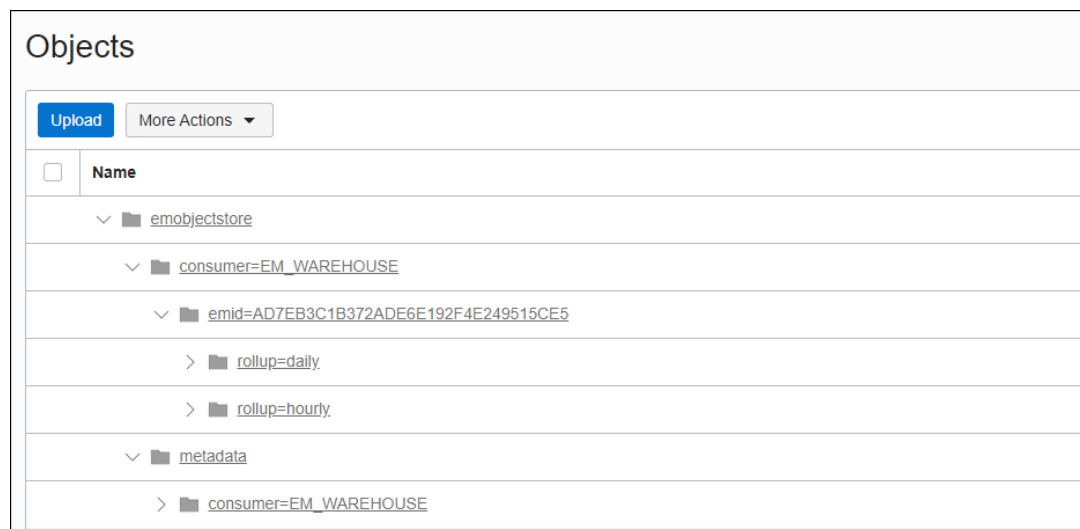
You can also configure a data warehouse. To do so, click **Warehouse**.

Enter the following to define the warehouse:

- Select the OCI Service.
- Select an OCI Bridge that has been created for the service.
- Select the Warehouse Database. Ensure that the Object Store Bucket and the Warehouse Database share a common OCI region for seamless data movement.
- Select the credential (named credential) used to access the Warehouse Database. A named credential can be created from the Enterprise Manager console (**Setup->Security->Named Credentials**).

Then, click **Configure** to configure a new warehouse connection.

3. Click **OK**.
4. Click **Enable Data Export**.
5. Under OCI Service, select a service type. For example *Ops Insights: EM Warehouse*.
6. Select the group you created in a prior step that contains all the targets for which you want data exported.
7. Select the Cloud Bridge and click **Submit**. Data from your Enterprise Manager instance should start uploading to the OCI bucket you defined.
8. In OCI, you can verify the data stored in your storage bucket. Navigate to *OCI Storage*, select **Buckets** and, in the compartment you created your bucket, click on the name of your bucket. The data in this bucket should look similar to the one shown below. Make a note of the name of your object store folder and emid.



Step 2: Import Data from the Object Storage Bucket to the OCI Service

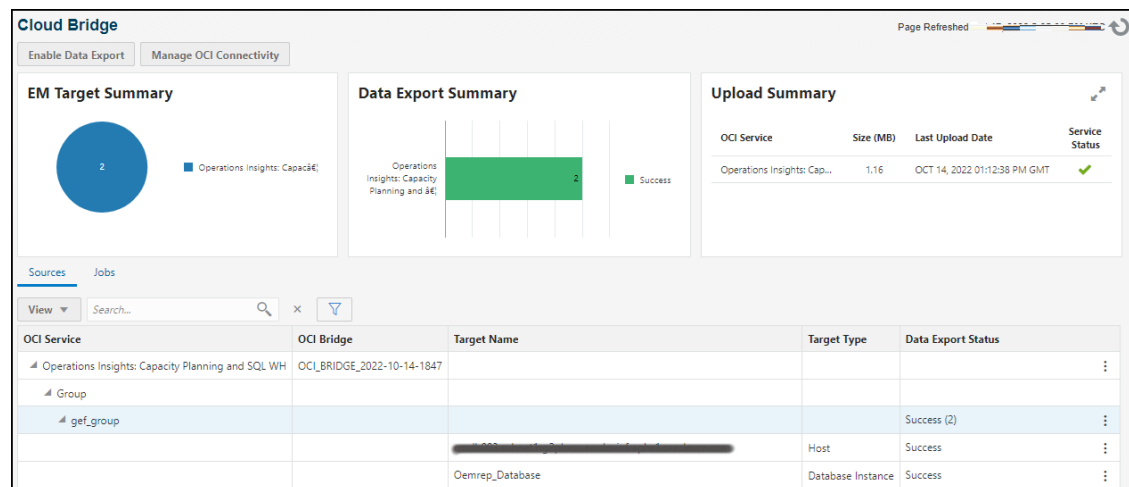
Once you've set up the Cloud Bridge to move data from Enterprise Manager to the OCI Object Storage bucket, you will need to create an *EM Bridge* to move Enterprise Manager target data from the Object Storage bucket to your OCI service for processing.

See your OCI service documentation for more information about importing Enterprise Manager target data.

Viewing Data Upload Status for a Service

Once you've successfully created an Cloud Bridge in Enterprise Manager and selected one or more target groups for data export to OCI, the *Cloud Bridge* dashboard will show the current upload status for each service including the groups that have been added for each service.

The *Summary* graphs display target upload rollup data for each OCI Service while the table provides a granular view of upload data for each service.



You can easily view which services are regularly uploading target data. Target data upload successes and failures appear in the *Data Export Status* column. The current data export status for each service is also shown in the *Upload Summary* region's *Service Status* column.

The following table shows all possible status conditions.

Table 11-1 Data Export Status

Status Condition	Description
Success	No errors for the source. The source is participating in data export.
Extract Error	Source has extraction errors. The source is participating in data export.
Transfer Error	Source has transfer errors. The source is participating in data export.
Load Error	Source has load errors. Source is participating in data export.
Data export paused at service	Data export paused at the OCI service level. Data export jobs are not running.
Group excluded from data export	Group is not participating in data export. Data export jobs are running.
Excluded from data export due to errors	Source has extraction errors and has been excluded from data export. The source is not participating in data export.
Source excluded from data export	Source is not participating in data export. Data export jobs are running.

You can also perform actions specific to the OCI service, target groups associated with that service, and individual target members of each group by clicking the vertical ellipsis in the Data Export Status column.

You can perform the following:

For an OCI Service, you can:

- Pause data export at the OCI service will stop/remove data export for that service. Restarting data export at the OCI service will start data export for the service.
- Restart/Pause data export for all relevant target groups associated with the selected OCI service to the OCI Object Storage bucket. Pausing data export at the OCI service will stop/remove data export for that service.
- Run Diagnostics: Enterprise Manager will run a series of diagnostics to check for problems that may have occurred with the target data export process as shown in the following graphic.

Data Export Diagnostics			
Name	Output	Result	Suggested User Action
Connectivity to OCI object store	Ok	✓	
Source EM availability summary	Pending/Unknown (3) Target Up (13)	✓	Use source or group level menu options, as applicable.
Source ETL status summary	Extract Paused (1) Success (17)	✓	Use source or group level menu options, as applicable.
Data export job	Scheduled	✓	
Data export job other extractor(s)	Scheduled	✓	
Data export errors	Extract failed. Check last job logs. (16-FEB-2021 10:15:15) Extract failed. Check last job	✓	Check log file for more details.

Note

Beginning with Oracle Enterprise Manager 13c Release 5 Update 10 (13.5.0.10), the diagnostics table can be downloaded as a CSV file using the Save As option.

- Show Errors from related entries in the OMS log files.
- Change the OCI Bridge currently being used by the service to a different OCI Bridge (*Modify OCI Bridge*). **Important:** Data export activity must be paused in order to switch to another OCI Bridge.
- Remove the OCI service.

For a target group, you can:

- Pause/Restart target group data export to the OCI Storage bucket. Pausing/restarting data export at the group level only excludes/includes the group involved in the data export. Data export jobs are not affected.
- Remove the Group

For any target within a group, you can:

- **Run Diagnostics:** Enterprise Manager will run a series of diagnostics on an individual target to check for problems that may have occurred with the target data export process, as shown in the following graphic.

Diagnostics - cloud-bridge-target-group			
Name	Output	Result	Suggested User Action
Target availability status	Ok	✓	None.
Preferred Host credential check	Ok	✓	None.
DB Monitoring credential check	Skipped	⚙️	Not applicable for the target type OR service.
OCI connectivity validation	Ok	✓	None.
DB Plug-in deployment status	Skipped	⚙️	Not applicable for the target type OR service.
Host preferred credential, user access validation	Ok	✓	None.
Cloud Bridge jar(s) availability on monitoring agent	Skipped	⚙️	Not applicable for the target type OR service.
OCI Service jar(s) availability on monitoring agent	Skipped	⚙️	Not applicable for the target type OR service.
Monitoring agent Host space availability check	Host : cloud-bridge-target-group om Space Available : 69%	✓	None.
Cloud Bridge proxy environment variable check	oci_http_proxy_host : oci_http_proxy_port :	ⓘ	Cloud Bridge proxy environment variable not set on the target host.
OCI OSS api invocation from monitoring agent	Ok	✓	None.
OCI OSS api invocation from monitoring agent via CURL	Input byte array has incorrect ending byte at 1592	✗	Make sure the proxy is set on the monitoring Agent host

- **Toggle Status:** You can start or stop individual target data export.
- **Show Errors**

Jobs

Whenever you click **Submit** to create an Cloud Bridge or add target groups for data export, an Enterprise Manager jobs are submitted to perform the requisite actions. If necessary, you can check on the status for all OCI-related jobs by clicking on the *Jobs* tab (located to the right of the *Sources* tab) to view explicit information about all jobs related to the management of EM Data for OCI Services.

Typically, you will not need this level of information. When you perform *Run Diagnostics* for a specific OCI service, all jobs associated with target data export are checked.

Monitoring Data Uploads from Enterprise Manager

Data export from Enterprise Manager to OCI is carried out by the Job System. There are, however, several conditions where the data export job may not run to completion. You can use Enterprise Manager's incident and event management functionality to monitor data export jobs.

Data export jobs can fail for several reasons:

1. Jobs can run into errors (system errors, Cloud Bridge issues, extractor related errors, etc.)
2. Data export jobs can be stopped or terminated from the Enterprise Manager Job System UI.
3. Data sources involved in the data export can run into problems due to availability, credential-related issues, and extract/transfer, or load-related errors.

Although all of these issues can be diagnosed via the *Run Diagnostic* function, you can take advantage of Enterprise Manager's native monitoring functionality (Incident Manager) to notify administrators immediately and correct the issue or possibly automate the problem resolution process.

In order to allow Enterprise Manager to monitor OCI data export jobs, a specialized target has been created called *Cloud Bridge Data Export* which can be monitored as a regular Enterprise Manager target.

Setting Up OCI Data Export Monitoring

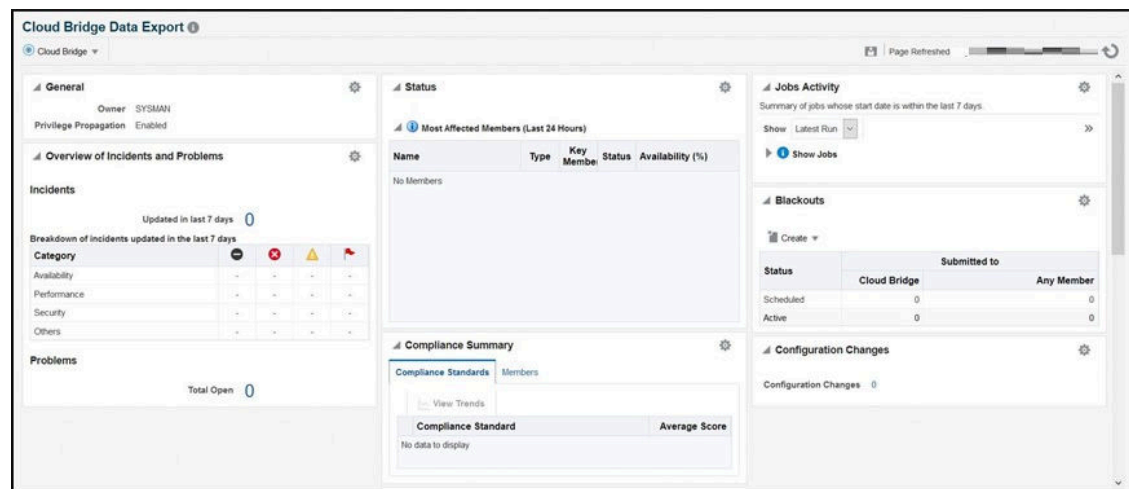
A *Cloud Bridge Data Export* target will be created automatically when data export is configured for at least one OCI service.

Note

The *Cloud Bridge Data Export* target will be automatically removed if there are no OCI services configured for data export job monitoring.

To view the target, navigate to the *All Targets* page (Targets->All Targets) and search for "bridge."

Click on the **Cloud Bridge Data Export** target in the list to view the target homepage.



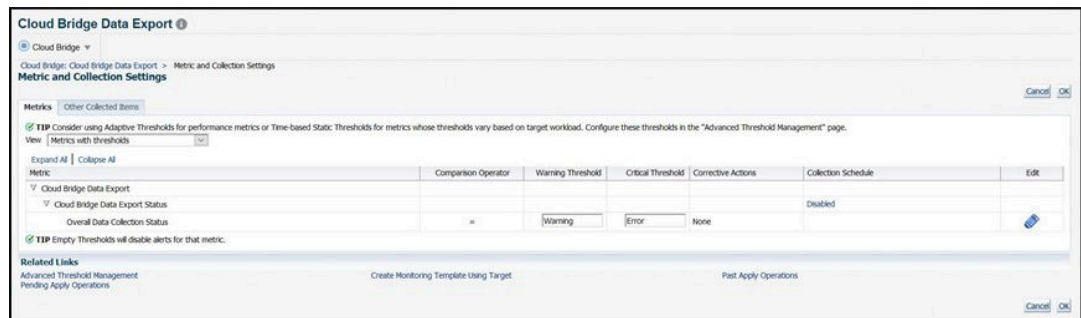
Note

If data export has not been configured for at least one OCI service, no target will appear.

Enable Metric Collection

Metrics are disabled out-of-box. Navigate to the *Metric and Collection Settings* page of the Cloud Bridge Data Export target.

1. From the Cloud Bridge drop-down menu, select **Monitoring** and then **Metric and Collection Settings**.

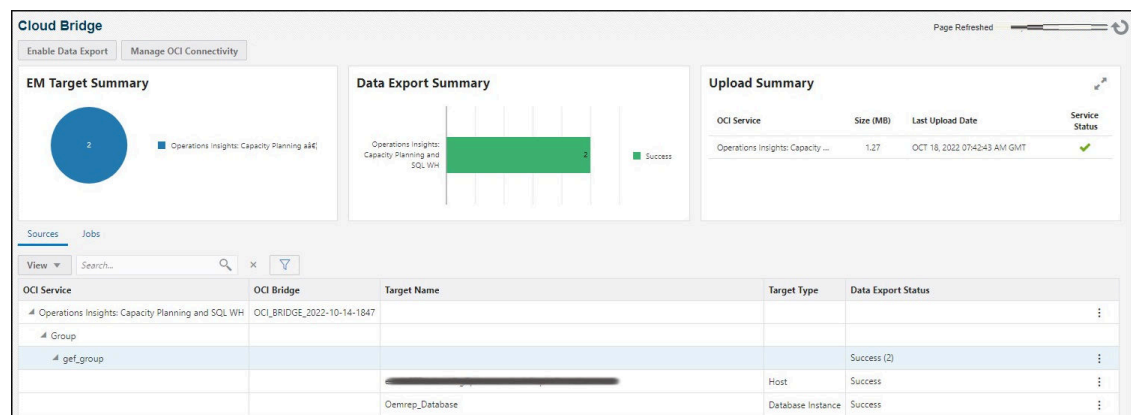


2. From the Collection Schedule column, click **Disabled**. The Edit Collection Settings page displays.
3. Click **Enable**.
4. Set the desired *Collection Frequency* and click **Continue**.
5. Click **OK**.

Monitoring Examples

An error occurs with an OCI service

The following graphic shows that a data upload error has occurred with an OCI service (Ops Insights).



An incident (Error) is raised

An incident will be raised when a data export job is stopped or removed.

Incident Manager: All open incidents Dashboard

Views: Search Actions View View search criteria Acknowledge Clear

Severity	Summary	Target	Priority	Status	Age	Time Since Last Update	Owner	Ackn	Escal	Type	Category	Ticket Type
Warning	Logging Analytics data export is running with Error. Diagnose the issue using Cloud Bridge dashboard.	Cloud Bri...	None	New	10 minutes	10 minutes	-	No	No	Incident	Unclassified	
Warning	Compliance score 33% is below critical threshold	Manage...	None	New	5 days 1 ...	5 days 1 hours	-	No	No	Incident	Unclassified	
Warning	Coherence Cache is Down	/EMOC...	None	New	5 days 1 ...	5 days 1 hours	-	No	No	Incident	Availability	

Rows Selected 1 Columns Hidden 23

Logging Analytics data export is running with Error. Diagnose the issue using Cloud Bridge dashboard. Open in new tab

Unassigned, Not acknowledged

General Events Notifications My Oracle Support Knowledge All Updates Related Events Related Metrics

Incident Details

ID 102

Metric Overall Data Collection Status

Metric Group Cloud Bridge Data Export Status

OCI Service log_analytics

Short Name Cloud Bridge Data Export (Cloud Bridge)

Target Cloud Bridge Data Export (Cloud Bridge)

Incident Created May 17, 2022 6:50:17 AM GMT+00:00

Last Updated May 17, 2022 6:50:17 AM GMT+00:00

Summary Logging Analytics data export is running with Error. Diagnose the issue using Cloud Bridge dashboard.

Internal Event data_export_status overall_dataexp_status

Tracking Acknowledge Add Comment Manage More

Escalated No

Priority None

Status New

Owner -

Acknowledged No

Last Incident created by rule (Name = Incident management rule set for all targets. Create incident for Comment: critical metric alert (System generated rule). on May 17, 2022 6:50:17 AM GMT+00:00)

This incident will be automatically cleared when the underlying issue is resolved.

Guided Resolution

Diagnostics Problem Analysis

Actions Reevaluate Alert

Corrective Actions No corrective action defined

An event is raised without an incident

An event without incident will be raised when:

- Data export is paused at the service level
- The source participating in data export is in error status

Cloud Bridge Data Export

Cloud Bridge

Cloud Bridge Data Export > All Metrics

All Metrics Search

View Cloud Bridge Data Export

Cloud Bridge Data Export Status

Collection Schedule Every 5 minutes

Upload Interval Every Collection

Last Upload May 17, 2022 7:06:16 AM GMT+00:00

OCI Service Short Name	Data Collection Status	OCI Service Name	Overall Data Collection Status	Overall Source Status
opsi	Warning	Operations Insights: Capacity Planning and SQL WH	Warning	Warning
log_analytics	Error	Logging Analytics	Error	Error

Data shown in above table is collected in real time.

Incident Manager: Events without incidents

Views: Search Actions View View search criteria Clear

Sever Message	Target Name	Target Type	Event Reported	Category	Last Updated	Incident ID
Operations Insights: Capacity Planning and SQL WH data export is running with Warning. Diagnose the issue using C...	Cloud Bridge	Cloud Bridge	May 17, 2022 7:0...	Unclassified	May 17, 2022 7:0...	
ERROR: failed executing jdeb348944495/oracle/bvencrisp em config -e node, 25 25 32512	Overrep_Dat...	Database In...	May 13, 2022 5:2...	Error	May 13, 2022 5:2...	
Enterprise Manager Minimum Database Setting Requirements are not met	Management...	OMS and Re...	May 13, 2022 5:1...	Unclassified	May 13, 2022 5:1...	

Rows Selected 1 Columns Hidden 17

Operations Insights: Capacity Planning and SQL WH data export is running with Warning. Diagnose the iss... Open in new tab Add Comment More

General Notifications My Oracle Support Knowledge All Updates History Related Events Related Metrics

Event Details

Metric Overall Data Collection Status

Metric Group Cloud Bridge Data Export Status

OCI Service opsi

Short Name Cloud Bridge Data Export (Cloud Bridge)

Target Cloud Bridge Data Export (Cloud Bridge)

Event Reported May 17, 2022 7:06:16 AM GMT+00:00

Last Updated May 17, 2022 7:06:17 AM GMT+00:00

Message Operations Insights: Capacity Planning and SQL WH data export is running with Warning. Diagnose the issue using Cloud Bridge dashboard.

Last Comment Operations Insights: Capacity Planning and SQL WH data export is running with Warning. Diagnose the issue using Cloud Bridge dashboard. on May 17, 2022 7:06:16 AM GMT+00:00

Internal Event Name data_export_status overall_dataexp_status

Internal Reported ...

Guided Resolution

Diagnostics Problem Analysis

Actions Reevaluate Alert

Corrective Actions No corrective action defined

This event will be automatically cleared when the underlying issue is resolved.

Adding Target Groups to OCI Services

Once the Cloud Bridge has been created, you can export additional Enterprise Manager target data for OCI service consumption by creating additional OCI service/target group pairings.

Navigate to the OCI Service Data Export dialog.

1. From the Setup menu, choose **Cloud Bridge**.
2. Click the **Enable Data Export** tab to display the OCI Service Data Export dialog.

When you select an OCI service, the associated Cloud Bridge is automatically selected. Simply select a new Source (target group) and click **Submit**.

Managing Cloud Bridges

You can create a new Cloud Bridge or edit/delete an existing bridge via the **Manage OCI Connectivity** dialog.

Navigate to the OCI Service Data Export dialog.

1. From the Setup menu, choose **Cloud Bridge**.
2. Click the **Manage OCI Connectivity** tab to display the Manage OCI Connectivity dialog.

Note

More than one OCI service can be associated with a single Cloud Bridge. Once a Cloud Bridge has been created for a service, it is no longer a selectable option from the **OCI Service** drop-down menu.

Viewing Cloud Extension Data

You can use Cloud Extension to view the Oracle Cloud Infrastructure (OCI) Ops Insights database details in Enterprise Manager.

Cloud Extension allows OCI [Ops Insights](#) database-specific insights, such as Capacity Planning and SQL Insights, to be displayed directly in Enterprise Manager interface under the database home page. You can view SQL performance insights, database capacity planning, and forecasting information in the context of a database, right on the Enterprise Manager's Database Resource page.

Cloud Extension is available starting with Enterprise Manager 13c Release 5 Update 23 (13.5.0.23).

- [Supported Oracle Database Types](#)
- [Configuring Cloud Extension](#)

Supported Oracle Database Types

Cloud Extension is available in the Enterprise Manager database home page of the following database types:

- Standalone (non-CDB)
- RAC database (non-CDB)

- PDB
- PDB on RAC

Note

Cloud Extension is not supported for the following database types: CDB, RAC instance, PDB on RAC instance, RAC database (CDB), Autonomous Database (ATP and ADW) and CDB\$ROOT.

Configuring Cloud Extension

You can configure Cloud Extension to be able to view Ops Insights database insights from the Enterprise Manager.

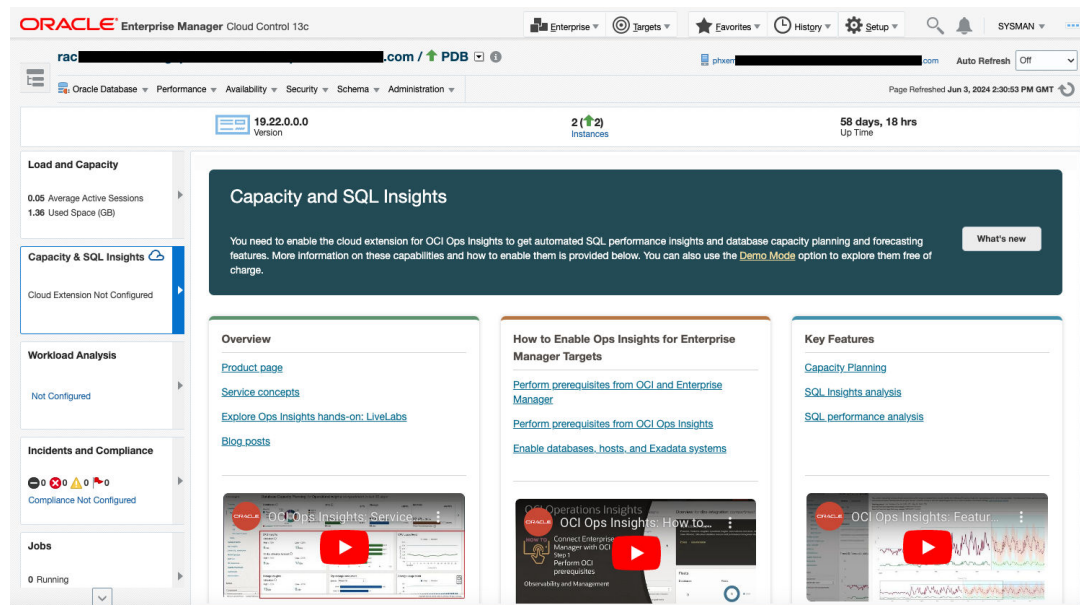
To configure Cloud Extension, do the following:

- Navigate to the Enterprise Manager database home page.
- From the left menu, click **Capacity & SQL Insights**.
The **Capacity and SQL Insights** pane is displayed on the right side.

The first time you click it, you can see the *"Cloud Extension Not Configured"* message on the left menu.

The **Capacity and SQL Insights** pane contains different resources, such as videos and documentation links, to assist you understanding the Ops Insights service and configuring Cloud Extension. It looks similar to the following:

Figure 11-1 Cloud Extension Not Configured



Alternatively, you can configure Cloud Extension by following the below steps:

1. Set up Enterprise Manager Cloud Bridge for OCI connectivity.
Use the Enterprise Manager Cloud Bridge to transfer data from Enterprise Manager to OCI Object Storage. For instructions, see:

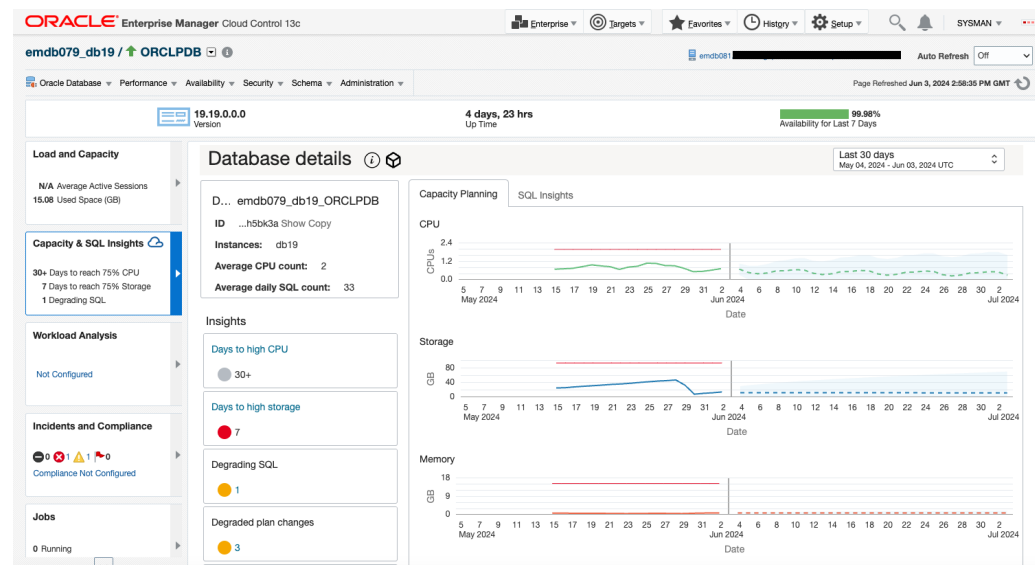
- [Prerequisites](#)
 - [Setting Up OCI Service Connectivity](#)
2. Enable the database in Ops Insights.
Use an Ops Insights EM Bridge to move data from the OCI Object Storage bucket to Ops Insights for analysis.

For instructions, see [Adding Enterprise Manager Targets](#) from *Ops Insights* documentation.
 3. Verify the configuration.
Navigate to the Enterprise Manager database home page and click **Capacity & SQL Insights** from the left side menu.

The **Database details** pane is displayed with the following tabs:

- **Capacity Planning**
It allows you to analyze and forecast database resource consumption using long-term historic data and machine learning. You can optimize resource usage by identifying and managing resource utilization, such as underutilized or over-utilized servers, and moving workloads, or adjusting resource allocations to maximize future performance. You can review out-of-the-box insights related to the capacity of the underlying infrastructure, such as CPU, storage, memory and I/O, and also see any outliers across these metrics for a given period and utilize auto ML-based forecasting algorithms to predict future demand of complex workloads.

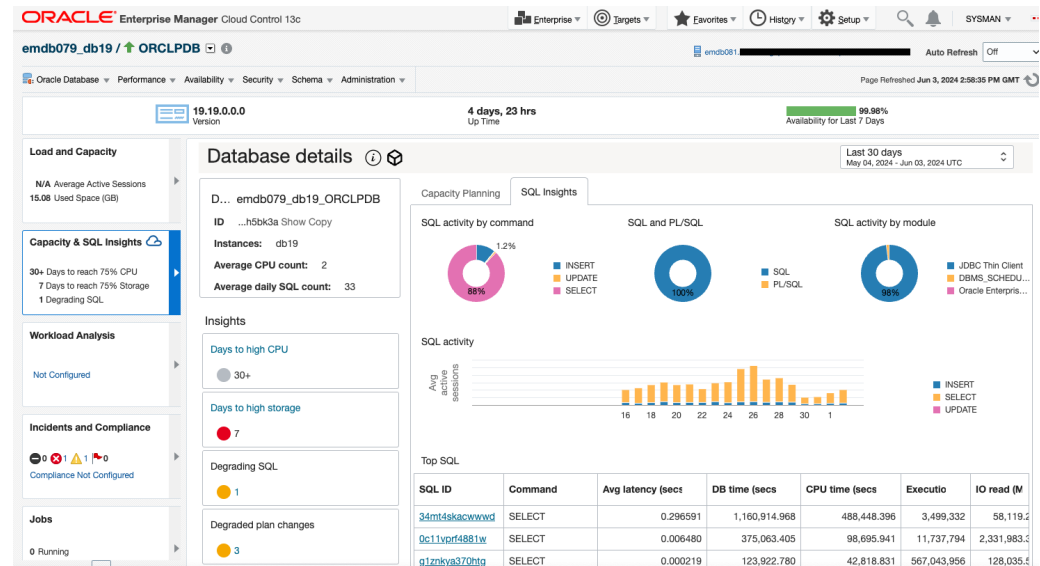
Figure 11-2 Ops Insights Capacity Planning



- **SQL Insights**
It provides a broad overview of the SQL workload executing in the database. This includes basic information about the database, such as version, cores and instances, and the SQL, such as unique and average daily counts, collected from the database. It also includes SQL activity breakdowns of total time by command and module, and the ratio of time in SQL or PL/SQL.

The **Insights** tiles at the database level quantify SQL by types of insights (degrading, degraded with plan changes, new, improving SQL and more). The SQL activity is shown by day, broken down by command type, exposing changes in workload over time. The charts: **Execute to parse ratio** and **SQL count and invalidations** expose important application workload characteristics over time.

Figure 11-3 Ops Insights SQL Insights



Note

The **Database details** pane is not displayed in the following scenarios:

- If Cloud Extension is not configured for the selected database, you see the **Capacity and SQL Insights** pane with resources and videos on Capacity Planning and SQL Insights. This scenario only happens if the initial configuration hasn't been completed.
- If the Enterprise Manager user you are logged in as doesn't have privileges to access Cloud Bridge, you see a landing page with resources and videos on Capacity Planning and SQL Insights.
- If the Enterprise Manager user you are logged in as doesn't have privileges to see performance information for the selected database. For example, the user only has view access to the database.
- If the selected database is configured for OCI in Enterprise Manager, but it's not enabled in OCI Ops Insights.
- If Cloud Bridge was configured correctly, but after the database was disabled or inactive, Enterprise Manager shows the following message: *Database Not Enabled for OCI Ops Insights*.
- If the browser has no external access available (no access to internet), you see the following message: *Unable to connect to OCI. Please check your internet connection or try again later*.

12

Generative AI Assistant

Learn about Ask EM, the Enterprise Manager Generative AI assistant, and its configuration.

Topics:

- [About Ask EM](#)
- [Configuring Ask EM](#)

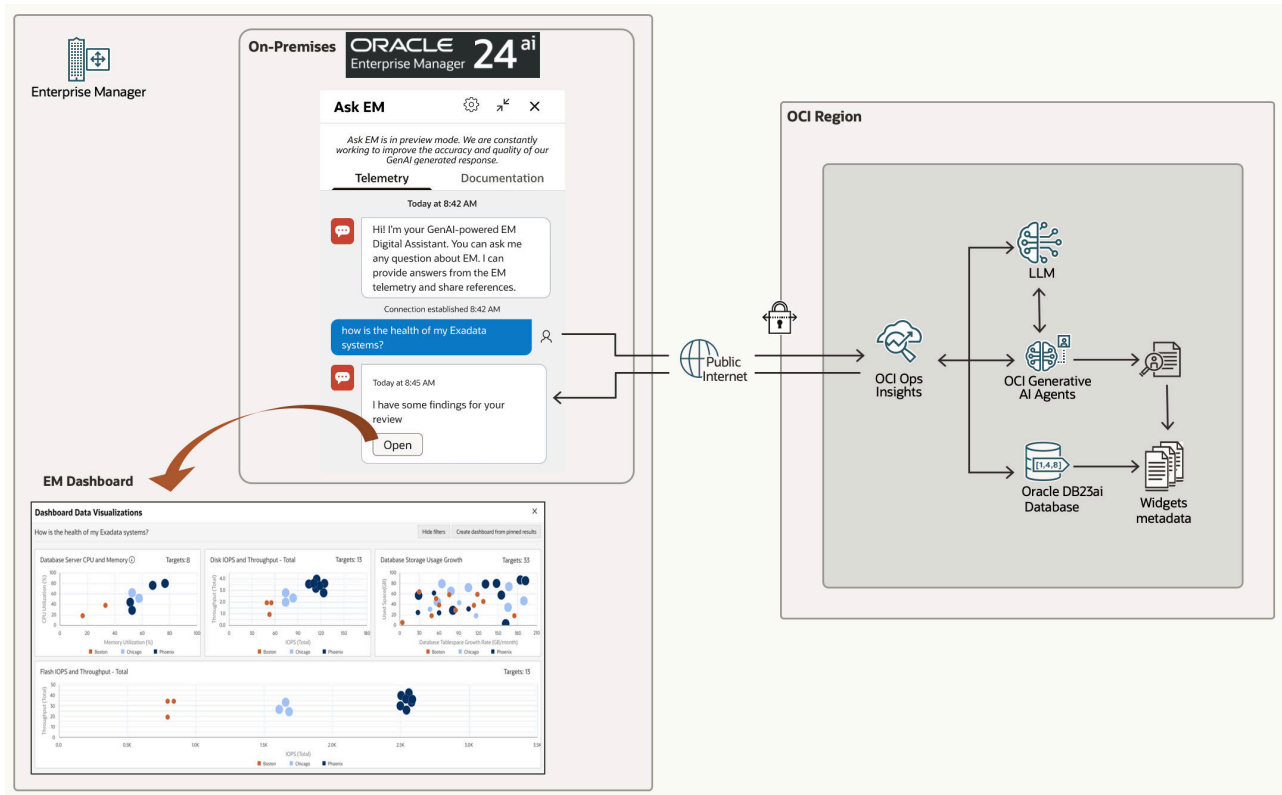
About Ask EM

Ask EM is the Enterprise Manager Generative AI assistant that covers different use cases, including chat and text generation, simplifying information discovery and increasing productivity.

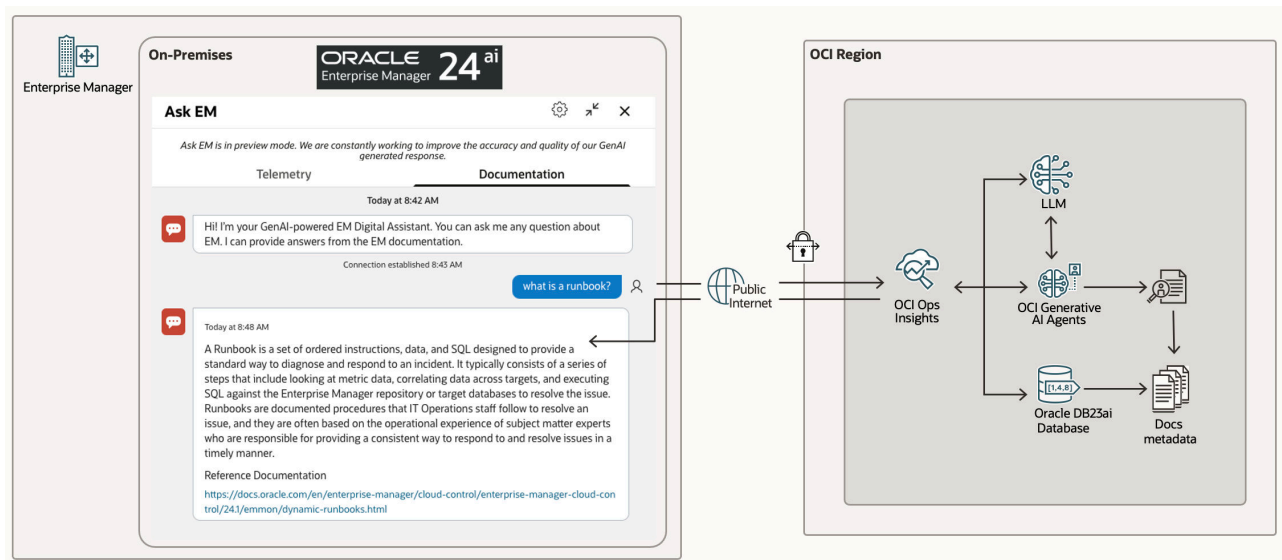
Starting with version 24.1, Oracle Enterprise Manager introduces the integration with OCI Generative AI service, delivering a powerful new solution called **Ask EM** for answering Enterprise Manager-related natural language queries. Ask EM leverages retrieval-augmented generation (RAG) technology to maximize response accuracy and relevance. The Gen AI assistant is specifically trained on the Enterprise Manager specific version of Enterprise Manager technical content, ensuring fast and reliable answers on a wide range of configuration, usage, and analysis questions.

Ask EM features two independent interfaces to streamline the user experience:

1. **Telemetry:** Provides direct links to relevant Enterprise Manager widgets and robust data visualization tools, enabling users to quickly access monitoring and analytic resources.




2. Documentation: Supplies direct access to pertinent sections of the comprehensive Enterprise Manager product documentation, supporting deeper exploration and learning.



With these capabilities, Ask EM simplifies information discovery and enhancing productivity for all Enterprise Manager users.

Configuring Ask EM

To configure Ask EM, perform the following steps:

1. Log into EM as Super Administrator and click on the Ask EM icon on the upper right hand corner  to automatically launch the setup wizard.
2. An [Oracle Cloud Account](#) in a [Gen AI region](#) and an [Ops Insights subscription](#) (enabled on a host or a database) are required.

If you are already a cloud customer, but not yet in a Gen AI region, see [Subscribing to an Infrastructure Region](#). Once you are logged in to your account, make a note of the following:

- a. Tenancy OCID. See [Finding Your Tenancy OCID](#) for more details.
 - b. User OCID. See [Finding Your User OCID](#) for more details.
 - c. Public Key Fingerprint. See [Finding Your Public Key Fingerprint](#) for more details.
 - d. Private Key Fingerprint. See [Finding Your Private Key Fingerprint](#) for more details.
3. Create a new OCI Named Credential or use an existing one. Use the values you noted above.
 4. Enable Auditing if you would like to audit session creation or termination. By default auditing is disabled.
 5. Select a [region where Gen AI](#) is enabled.
 6. Test Connection and Save.
 7. By default, all Super Administrators are provided with the EM_ASKEM_ADMIN role. Optionally, you can grant the EM_ASKEM_ADMIN role to all Administrators you would like to have access to Ask EM and then save it. These EM Administrators will have access to both the Telemetry and Documentation interfaces.

As a Super Administrator, you have the ability to configure granular access controls for Ask EM. Using **Resource Privileges**, you can specify whether individual users have access to only the Telemetry tab, only the Documentation tab, or both. For example, to restrict a user's access to just the Ask EM Documentation interface, create or edit an Administrator account, navigate to **Other Resource Privileges**, and, under the resource type: Ask EM Assistant, assign the **Documentation** privilege.

By default the Ask EM interface is enabled in Enterprise Manager.

To disable it, run the following command on the primary OMS host:

```
emctl set property -name enable_genai_assistant -value false
```

To re-enable it, run the following command on the primary OMS host:

```
emctl set property -name enable_genai_assistant -value true
```

Part III

Generating Reports

Enterprise Manager provides multiple ways to view information about managed targets.

This section contains the following chapters:

- [Controlling Resource Usage](#)
- [Creating Dashboards Using Grafana](#)
- [Using Information Publisher](#)
- [Standalone Oracle Analytics Server](#)

Controlling Resource Usage

In order to protect the performance of key Enterprise Manager subsystems, it has been designed to limit overuse of API end-points that could negatively impact performance. To limit any impact reporting may have on the performance of key Enterprise Manager subsystems, two new features have been added giving Enterprise Manager administrators more control over the resources reporting tasks may consume. These features are:

- [Repository Session \(SQL\) Throttling](#): Resource management on the database containing the Oracle Enterprise Manager Repository.
- [Application API Throttling](#): Application API throttling on the Oracle Management Server. You set OMS properties to limit the number of concurrent API requests being executed by the OMS.

Note

Application API throttling only applies to Grafana dashboard creation.

Repository Session (SQL) Throttling

You can run SQL to extract report data when using any of the Enterprise Manager reporting framework options:

- Information Publisher
- Grafana Dashboards
- Metric Extractor

or when using Dynamic Runbooks.

Running SQL queries against Enterprise Manager could potentially impact operational performance, so to ensure the performance of Enterprise Managers core systems you can use Database Resource Manager. Database Resource Manager gives the Oracle Database server more control over resource management decisions, thus circumventing problems resulting from inefficient operating system management.

In addition to potential load on the Enterprise Manager repository from Grafana, other reporting options, such as Information Publisher and OMC Collector, also have the potential to impact performance. The Database Resource Manager can be configured to ensure that any impact is contained and does not impact operational performance of Enterprise Manager itself.

Area	Module
Information Publisher	EMIP_REPORTS
Grafana	Grafana
OMC Collector	DATA_COLLECTOR
Execute SQL REST API	executeSQL
Metric Extractor	METRIC_EXTRACTOR
Console	ORACLE_NAMED_QUERY

Area	Module
Console	EM_FREE_FORM_QUERY, EM_FREE_FORM_QUERY_DASHBOARDS, EM_EXEC_SQL_RUNBOOKS

Using Database Resource Manager requires that you create a Resource Manager Plan. Enterprise Manager comes with a Resource Manager Plan that can be used to limit resource usage at a database or PDB level. See [Applying the Resource Manager Plan](#) for information about the default Resource Manager Plan for the Reporting Framework.

By default, this plan will only limit Grafana connections to 2% of a database host's CPU. Throttling for other reporting options is off (commented out) by default. To enable throttling for these areas, uncomment the following lines in this file.

For Information Publisher Reports

```
DBMS_RESOURCE_MANAGER.SET_CONSUMER_GROUP_MAPPING
(DBMS_RESOURCE_MANAGER.MODULE_NAME, 'EMIP_REPORTS', 'EM_REPORTS_GROUP');
```

For Dynamic Runbooks

```
DBMS_RESOURCE_MANAGER.SET_CONSUMER_GROUP_MAPPING
(DBMS_RESOURCE_MANAGER.MODULE_NAME, 'EM_EXEC_SQL_RUNBOOKS',
'EM_REPORTS_GROUP');
```

Applying the Resource Manager Plan

To apply the Resource Manager Plan, you need to run the `admin_create_resmgr_plan.sql` via Database Resource Manager.

The default Resource Manager Plan is located at the following location.

```
$ORACLE_HOME/sysman/admin/emdrep/sql/core/latest/admin/
admin_create_resmgr_plan.sql
```

To execute this plan, you must have the system privilege `ADMINISTER_RESOURCE_MANAGER` to administer the Resource Manager. This privilege (with the `ADMIN` option) is granted to database administrators through the `DBA` role. For information about using Database Resource Manager, see [Managing Resources with Oracle Database Resource Manager](#).

Use Caution: Applying the `admin_create_resmgr_plan.sql` Resource Manager Plan will overwrite any existing Resource Manager Plans that may be in effect.

To verify that the plan execution has been applied, run the following:

```
show parameter RESOURCE_MANAGER_PLAN
```

`RESOURCE_MANAGER_PLAN` will be set to `EM_REPORTS_HARD_CPU_LIMIT` upon successful plan execution.

A metric is added to the `oracle_emrep` target to track when throttling happens. The metric name is *Resource Manager Statistics*. This metric tracks when CPU throttling is happening per database/PDB instance.

Removing the Resource Manager Plan

To remove the Resource Manager Plan, run the following SQL script:

```
$ORACLE_HOME/sysman/admin/emdrep/sql/core/latest/admin/  
admin_drop_resmgr_plan.sql
```

Application API Throttling

To protect the Enterprise Manager OMS against an excessive amount of resource usage, you can set the following OMS properties that govern the throttling effect.

Note

Application API throttling only applies to Grafana dashboard creation.

Depending on the version of Enterprise Manager you are running, OMS properties will be different. The following tables list OMS throttling properties that can be used for specific Enterprise Manager releases.

Table 13-1 OMS Throttling Setting Properties (Release 6 and greater)

Property Name	Data Type	Default Value	Purpose	Error Message
oracle.sysman.db.restfulapi.grafana.throttle.max.concurrent.request	number	20	Global Limit Control the total number of concurrent requests per OMS.	You have hit the API's maximum number of concurrent access limit of <oracle.sysman.db.restfulapi.grafana.throttle.max.concurrent.request> . Contact Enterprise Manager Administrator to adjust this limit.
oracle.sysman.db.restfulapi.grafana.throttle.max.request.per.user	number	30	Per-user Limit Control the total number of concurrent requests per user and per OMS.	You have exceeded the limit of <oracle.sysman.db.restfulapi.grafana.throttle.max.request.per.user> API requests per <oracle.sysman.db.restfulapi.grafana.throttle.max.request.per.user.interval.seconds> seconds. You can reduce the page refresh frequency or Contact Enterprise Manager Administrator to adjust this limit.

Table 13-1 (Cont.) OMS Throttling Setting Properties (Release 6 and greater)

Property Name	Data Type	Default Value	Purpose	Error Message
oracle.sysman.db.restfulapi.grafana.throttle.max.request.per.user.interval.seconds	number	60 (seconds)	Rate-limiting Control the rate at which the user can access the API, i.e., within a 10 minute window, the maximum number of API requests a single user can make.	You have exceeded the limit of <oracle.sysman.db.restfulapi.grafana.throttle.max.request.per.user> API requests per <oracle.sysman.db.restfulapi.grafana.throttle.max.request.per.user.interval.seconds> seconds. You can reduce the page refresh frequency or Contact Enterprise Manager Administrator to adjust this limit.
oracle.sysman.db.restfulapi.grafana.timeseries.maxdatapoints	number	10000	Data Limit Determines the maximum number of datapoints to return when any query is executed for Grafana Plugin's Timeseries Query Type option.	None, number of rows in the query result will be simply be reduced to the maximum value set.
oracle.sysman.db.restfulapi.grafana.timeseries.maxnumrows	number	100	Data Limit Determines the maximum number of rows to return when any query is executed for Grafana Plugin's Non-timeseries Query Type option.	None, number of rows in the query result will be simply be reduced to the maximum value set.
oracle.sysman.db.restfulapi.grafana.timeseries.maxnumcolumns	number	10	Data Limit Determines the maximum number of columns to return when any query is executed for Grafana Plugin's Non-timeseries Query Type option.	None, number of columns in the query result will be simply be reduced to the maximum value set.
oracle.sysman.db.restfulapi.grafana.query.timeout	number	180 (seconds)	Query Timeout Limits the amount of time (in seconds) a query execution can spend on a database. Default is 180 seconds.	Query execution was interrupted, maximum statement execution time(" +queryTimeout+ " seconds) exceeded.

The following OMS properties are used with Enterprise Manager Release 4 and Release 5.

Table 13-2 OMS Throttling Setting Properties (Release 4 and Release 5)

Property Name	Data Type	Default Value	Purpose	Error Message
<code>oracle.sysman.db.restfulapi.grafana.throttle.max.concurrent.request</code>	number	20	Global Limit Control the total number of concurrent requests per OMS.	You have hit the API's maximum number of concurrent access limit of < oracle.sysman.db.restfulapi.grafana.throttle.max.concurrent.request >. Contact Enterprise Manager Administrator to adjust this limit.
<code>oracle.sysman.db.restfulapi.grafana.throttle.max.request.per.user</code>	number	30	Per-user Limit Control the total number of concurrent requests per user and per OMS.	You have exceeded the limit of < oracle.sysman.db.restfulapi.grafana.throttle.max.request.per.user > API requests per < oracle.sysman.db.restfulapi.grafana.throttle.max.request.per.user.interval.seconds > seconds. You can reduce the page refresh frequency or contact an Enterprise Manager Administrator to adjust this limit.
<code>oracle.sysman.db.restfulapi.grafana.throttle.max.request.per.user.interval.seconds</code>	number	60 (seconds)	Rate-limiting Control the rate at which the user can access the API, i.e., within a 10 minute window, the maximum number of API requests a single user can make.	You have exceeded the limit of < oracle.sysman.db.restfulapi.grafana.throttle.max.request.per.user > API requests per < oracle.sysman.db.restfulapi.grafana.throttle.max.request.per.user.interval.seconds > seconds. You can reduce the page refresh frequency or contact an Enterprise Manager Administrator to adjust this limit.

Table 13-2 (Cont.) OMS Throttling Setting Properties (Release 4 and Release 5)

Property Name	Data Type	Default Value	Purpose	Error Message
oracle.sysman.db.restfulapi.grafana.executecutesql.repository.query.timeout	number	180 (seconds)	Query Timeout Limits the amount of time (in seconds) a query execution can spend on a repository.	Query execution was interrupted, maximum statement execution time("+queryTimeout+" seconds) exceeded.
oracle.sysman.db.restfulapi.grafana.executecutesql.target.query.timeout	number	180 (seconds)	Query Timeout Limits the amount of time (in seconds) a query execution can spend on a database.	Query execution was interrupted, maximum statement execution time("+queryTimeout+" seconds) exceeded.

You can set these OMS properties using EMCTL as shown in the following examples.

```
emctl set property -name
oracle.sysman.db.restfulapi.grafana.throttle.max.concurrent.request -value 5 -
sysman_pwd <pwd>
emctl set property -name
oracle.sysman.db.restfulapi.grafana.throttle.max.req.per.user -value 10 -
sysman_pwd <pwd>
emctl set property -name
oracle.sysman.db.restfulapi.grafana.throttle.max.req.per.user.interval.sec -
value 120 -sysman_pwd <pwd>
```

Alternatively, you can view and edit OMS properties from the Enterprise Manager console as follows:

1. From the **Setup** menu, select **Manage Enterprise Manager**, then select **Management Services**.

Note

You will need *OMS Configuration Property* resource privilege to navigate to this page.

2. On the Management Services page, click **Configuration Properties**.
3. On the Configuration Properties page, you can view and edit OMS properties.

Repository Session (SQL) Throttling

To protect the Enterprise Manager Repository database, you can control the number of SQL requests. This type of throttling is carried out at the database level using the Database Resource Manager. For information about limiting SQL requests, see [Repository Session \(SQL\) Throttling](#).

Creating Dashboards Using Grafana

Grafana is an open source technology used for metric analytics & visualization. The Oracle Enterprise Manager App for Grafana allows you to integrate Enterprise Manager metric data (collected from multiple managed targets and stored in the Enterprise Manager repository) with any other data sources you have access to.

By adding the Oracle Enterprise Manager App for Grafana, you can extract OMS repository metric data and display it graphically for fast, intuitive access to performance and metric information. You can create custom Enterprise Manager-based Grafana dashboards by simply browsing and selecting the Enterprise Manager metrics of interest, or running simple SQL queries against the Enterprise Manager repository tables, without a deep knowledge of the Enterprise Manager data model. Data from multiple Enterprise Manager sites, along with data from other data sources, can be easily displayed on a single dashboard.

For more information about enabling the Oracle Enterprise Manager App for Grafana, see [Enable the Oracle Enterprise Manager App for Grafana](#).

Using Information Publisher

Information Publisher, Enterprise Manager's reporting framework, makes information about your managed environment available to audiences across your enterprise. Strategically, reports are used to present a view of enterprise monitoring information for business intelligence purposes, but can also serve an administrative role by showing activity, resource utilization, and configuration of managed targets. IT managers can use reports to show availability of sets of managed systems. Executives can view reports on availability of applications (such as corporate email) over a period of time.

The reporting framework allows you to create and publish customized reports: Intuitive HTML-based reports can be published via the Web, stored, or e-mailed to selected recipients. Information Publisher comes with a comprehensive library of predefined reports that allow you to generate reports out-of-box without additional setup and configuration.

This chapter covers the following topics:

- [About Information Publisher](#)
- [Out-of-Box Report Definitions](#)
- [Custom Reports](#)
- [Scheduling Reports](#)
- [Sharing Reports](#)

About Information Publisher

Information Publisher provides powerful reporting and publishing capability. Information Publisher reports present an intuitive interface to critical decision-making information stored in the Management Repository while ensuring the security of this information by taking advantage of Enterprise Manager's security and access control.

Information Publisher's intuitive user-interface allows you to create and publish reports with little effort. The key benefits of using Information Publisher are:

- Provides a framework for creating content-rich, well-formatted HTML reports based on Management Repository data.
- Out-of-box reports let you start generating reports immediately without any system configuration or setup.
- Ability to schedule automatic generation of reports and store scheduled copies and/or e-mail them to intended audiences.
- Ability for Enterprise Manager administrators to share reports with the entire business community: executives, customers, and other Enterprise Manager administrators.

Information Publisher provides you with a feature-rich framework that is your central information source for your enterprise.

Out-of-Box Report Definitions

The focal point of Information Publisher is the report definition. A report definition tells the reporting framework how to generate a specific report by defining report properties such as report content, user access, and scheduling of report generation.

Information Publisher comes with a comprehensive library of predefined report definitions, allowing you to generate fully formatted HTML reports presenting critical operations and business information without any additional configuration or setup. .

Generating this HTML report involved three simple steps:

Step 1: Click **Availability History** (Group) in the report definition list.

Step 2: Select the group for which you want to run the report.

Step 3: Click **Continue** to generate the fully-formed report.

Supplied report definitions are organized by functional category with each category covering key areas.

To access the Information Publisher home page, from the **Enterprise** menu, choose **Reports** and then **Information Publisher**.

Custom Reports

Although the predefined report definitions that come with Information Publisher cover the most common reporting needs, you may want to create specialized reports. If a predefined report comes close to meeting your information requirements, but not quite, you can use Information Publisher's Create Like function to create a new report definition based on one of the existing reports definitions.

Creating Custom Reports

To create custom reports:

1. Choose whether to modify an existing report definition or start from scratch. If an existing report definition closely matches your needs, it is easy to customize it by using the Create Like function.
2. Specify name, category, and sub-category. Enterprise Manager provides default categories and sub-categories that are used for out-of-box reports. However, you can categorize custom reports in any way you like.
3. Specify any time-period and/or target parameters. The report viewer will be prompted for these parameters while viewing the report.
4. Add reporting elements. Reporting elements are pre-defined content building blocks, that allow you to add a variety of information to your report. Some examples of reporting elements are charts, tables, and images.
5. Customize the report layout. Once you have assembled the reporting elements, you can customize the layout of the report.

Report Parameters

By declaring report parameters, you allow the user to control what data is shown in the report. There are two types of parameters: target and time-period.

Example: If you are defining a report that will be used to diagnose a problem (such as a memory consumption report), the viewer will be able to see information for their target of interest.

By specifying the time-period parameter, the viewer will be able to analyze historical data for their period of interest.

Analyzing Historical Data

Information Publisher allows you to view reports for a variety of time-periods:

- Last 24 Hours/ 7 Days/ 31 Days
- Previous X Days/ Weeks/ Months/ Years (calendar units)
- This Week/ This Month/ This Year (this week so far)
- Any custom date range.

Report Elements

Report elements are the building blocks of a report definition. In general, report elements take parameters to generate viewable information. For example, the Chart from SQL element takes a SQL query to extract data from the Management Repository and a parameter specifying whether to display the data in the form of a pie, bar, or line chart. Report elements let you "assemble" a custom report definition using the Information Publisher user interface.

Information Publisher provides a variety of reporting elements. Generic reporting elements allow you to display any desired information, in the form of charts, tables or images. For example, you can include your corporate Logo, with a link to your corporate Web site. Monitoring elements show monitoring information, such as availability and alerts for managed targets. Service Level Reporting elements show availability, performance, usage and achieved service levels, allowing you to track compliance with Service Level Agreements, as well as share information about achieved service levels with your customers and business executives.

Scheduling Reports

Enterprise manager allows you to view reports interactively and/or schedule generation of reports on a flexible schedule. For example, you might want to generate an "Inventory Snapshot" report of all of the servers in your environment every day at midnight.

Flexible Schedules

Enterprise Manager provides the following scheduling options:

- One-time report generation either immediately or at any point in the future
- Periodic report generation
 - Frequency: Any number of Minutes/ Hours/ Days/ Weeks/ Months/ Years
 - You can generate copies indefinitely or until a specific date in the future.

Storing and Purging Report Copies

Enterprise Manager allows you to store any number of scheduled copies for future reference. You can delete each stored copy manually or you can set up automated purging based on either the number of stored copies or based on retention time. For example, you can have Enterprise Manager purge all reports that are more than 90 days old.

E-mailing Reports

You can choose for scheduled reports to be e-mailed to any number of recipients. You can specify reply-to address and subject of the e-mail.

Sharing Reports

Information Publisher facilitates easy report sharing with the entire user community. Enterprise Manager administrators can share reports with other administrators and roles. However, there may be cases when you need to share reports with non-Enterprise Manager administrators, such as customers and/or business executives. To facilitate information sharing with these users, Enterprise Manager renders a separate reporting Web site that does not require user authentication.

Note

To ensure that no sensitive information is compromised, only Enterprise Manager administrators with a special system privilege are allowed to publish reports to the Enterprise Manager reports Web site.

Information Publisher honors Enterprise Manager roles and privileges, ensuring that only Enterprise Manager administrators can create reports on the information they are allowed to see. When sharing reports, administrators have an option of allowing report viewers to see the report with the owner's privileges. For example, as a system administrator you might want to share a host's performance information with a DBA using your server, but you do not want to grant the DBA any privileges on your host target. In this case, you could create a host performance report, and allow the DBA to view it with your privileges. This way, they only see the information you want them to see, without having access to the host homepage.

Standalone Oracle Analytics Server

Beginning with Oracle Enterprise Manager 13c Release 5 (13.5), embedded BI Publisher reporting functionality is no longer available from the Enterprise Manager console.

If you want to use BI Publisher reporting functionality, you will need to install/access a standalone instance of Oracle Analytics Server (OAS), previously called Oracle Business Intelligence Enterprise Edition (OBIEE). Similarly, BI Publisher, which is part of OBIEE, has been renamed Oracle Analytics Publisher (OAP). Detailed instructions for installing and configuring a standalone OAS/OAP system are documented in the [Oracle Analytics Server Technical Brief](#).

By using a standalone OAS deployment for your reporting needs, you'll have the flexibility to update reporting functionality independent of Enterprise Manager installation, upgrade, and patch cycles.

Index

A

- Accessing Plug-In Manager, [8](#)
- accessing Software Library Administration page, [8](#)
- accessing Software Library console, [1](#)
- Add HTTP Location, [15](#)
- Add NFS Location, [15](#)
- Add OMS Agent file system, [14](#)
- Add OMS Agent file system location, [15](#)
- Add OMS Shared file system, [12](#)
- adding targets, [7](#)
- Agents, updating, [7](#)
- aggregation and purging policies
 - See data retention policies, [2](#)
- archive logging
 - for Management Repository database, [1](#)
- auditing
 - enabling, [2](#)
- automated patching
 - Offline mode, [65](#)
 - Online mode, [65](#)
- automated patching advantages, [65](#)
- Availability History Report, picture of, [2](#)

B

- benefits of Information Publisher, [1](#)

C

- catalog archives, [15](#)
- configuring Services
 - availability
 - beacons, [3](#)
 - key beacons, [3](#)
- Command Line Interface, [28](#)
- creating, [2](#)
- metrics
 - usage, [15](#)
- monitoring settings, [9](#)
 - beacon overrides, [9](#)
 - Collection Settings tab, [9](#)
 - Data Granularity property, [10](#)
 - frequency, [9](#)
- performance metrics, [13](#)
 - aggregation function, [14](#)

- configuring Services (*continued*)

- Root Cause Analysis, [8](#)
 - Topology page, [8](#)
 - Service Level Rules, [26](#)
 - actual service level, [27](#)
 - availability, [26](#)
 - business hours, [26](#)
 - expected service level, [27](#)
 - Information Publisher, [28](#)
 - performance criteria, [26](#)
 - Services Dashboard, [28](#)
 - service test-based availability
 - key service tests, [7](#)
 - service tests and beacons
 - configuring dedicated beacons, [12](#)
 - configuring Web proxy, [12](#)
 - selecting test type, [10](#)
- configuring Software Library, [1](#)
 - administrators privileges, [2](#)
 - installation procedure, [12](#)
 - OMS Agent storage, [13](#)
 - OMS shared file system, [12](#)
 - referenced storage location, [15](#)
 - maintenance procedure, [35](#)
 - deleting Software Library storage location., [36](#)
 - periodic maintenance tasks, [35](#)
 - re-importing Oracle owned entity files, [36](#)
- overview, [1](#)
- prerequisites, [11](#)
- roles and Software Library privileges, [2](#)
- storage, [7](#)
 - user roles and privileges, [2](#)

- connect descriptor, [10](#)
- using to identify the Management Repository database, [10](#)
- creating
- custom reports, [2](#)
- report definitions, [2](#)
- custom reports, [2](#)
- customizing Enterprise Manager pages, [1](#)

D

- data
 - aggregating, [3](#)

data (*continued*)
 purging, [3](#)
 data purge policy, [4](#)
 data retention policies
 for Application Performance Management
 data, [2](#)
 Management data, [4](#)
 Management Repository, [2](#)
 modifying default, [5](#)
 database
 insufficient memory, [8](#)
 database scheduler
 troubleshooting, [7](#)
 dbms_scheduler, [7](#)
 allowed sessions, [8](#)
 disabling, [8](#)
 DBMS_SCHEDULER
 troubleshooting, [7](#)
 default aggregation, [2](#)
 deploying plug-ins, [17](#), [21](#)
 deployment, [4](#)
 deployment plug-ins, [21](#)
 deployment status, [22](#)
 discovering targets, [6](#)
 disk mirroring and stripping
 Management Repository guideline, [1](#)
 disk space management
 controlling the size and number of log and
 trace files, [17](#)
 controlling the size of log and trace files, [18](#)
 downloading logs, [7](#)
 downloading plug-ins, [14](#), [15](#)
 drop command, [9](#)
 dropping the Management Repository, [9](#)

E

EMCLI, setting up, [4](#)
 emctl commands
 Management Agent, [12](#)
 EMCTL Commands for OMS, [7](#)
 emctl reload, [13](#)
 emctl upload, [13](#)
 emctl.log, [17](#)
 emctl.log file, [30](#)
 emoms_pbs.trc, [16](#)
 emoms.log, [17](#)
 emomslogging.properties
 MaxBackupIndex, [18](#)
 MaxFileSize, [18](#)
 Enterprise Manager
 starting, [2](#)
 starting all components of, [2](#)
 Enterprise Manager, maintaining, [1](#)
 events
 historical data, [4](#)

extensibility paradigm, [2](#)

G

gcagent_errors.log, [11](#)
 generating HTML reports, [2](#)
 Grid Control
 stopping, [3](#)
 stopping all components of, [3](#)

H

Health Overview, [2](#)
 home page
 setting, [2](#)

I

Information Publisher
 Create Like function, [2](#)
 generating HTML reports, [2](#)
 overview of, [1](#)
 report
 definitions, [2](#)
 elements, [3](#)
 reporting framework, [1](#)
 sharing reports, [4](#)
 viewing reports, [4](#)
 informational updates, [6](#)

J

job slave processes, [7](#)
 job_queue_processes, [7](#)
 jobs
 modifying retention period, [6](#)

L

local store, [3](#)
 log files
 controlling the size and number of, [17](#)
 locating and configuring, [1](#)
 locating Management Agent, [11](#)
 locating Management Service, [17](#)
 Management Agent, [10](#)
 Oracle Management Service, [16](#)
 searching, [5](#)
 log4j.appender.emlogAppender.
 MaxBackupIndex, [18](#)
 log4j.appender.emlogAppender. MaxFileSize, [18](#)
 log4j.appender.emtrcAppender. MaxBackupIndex,
 [18](#)
 log4j.appender.emtrcAppender. MaxFileSize, [18](#)
 LVM (Logical Volume Manager), [1](#)

M

Management Agent, [10](#)
 Management Agent logs
 setting log levels, [12–14](#)
 setting trace levels, [16](#)
 Management Repository, [2](#)
 creating, [10](#)
 deployment guidelines, [1](#)
 dropping, [9](#)
 migration, [13](#)
 migration prerequisites, [15, 18](#)
 recreating, [9](#)
 removing, [9](#)
 server connection hung error, [11](#)
 troubleshooting, [11, 12](#)
 Management Service
 starting and stopping on Windows systems, [4](#)
 managing logs, [1](#)
 MAX_UTILIZATION, [8](#)
 MaxBackupIndex
 property in emomslogging.properties, [18](#)
 MaxFileSize
 property in emomslogging.properties, [18](#)
 MGMT_METRICS_1DAY table, [5](#)
 MGMT_METRICS_1HOUR table, [5](#)
 MGMT_METRICS_RAW table, [5](#)
 Migrating, [36](#)
 migration
 post migration troubleshooting, [31](#)
 post migration verification, [28](#)
 repository, [15, 18](#)
 repository methodologies, [15, 17–22, 24, 25, 27](#)
 modes of patching, [65](#)
 monitoring credentials
 defined, [7](#)
 setting, [6](#)
 My Oracle Support, OMS Patches, [15](#)
 My Oracle Support, OPatchauto, [15](#)

N

new product announcements, [6](#)

O

Offline mode, [65](#)
 OMS
 emctl commands, [7](#)
 OMS Configurations, OPatchauto, [8](#)
 OMS Configurations, OPatchauto, [8](#)
 OMSPatcher, prerequisites, [14](#)
 Online mode, [65](#)
 opatchauto lspatches, [35](#)
 OPatchauto Parameters, [11](#)

OPatchauto Property File, [11](#)
 opatchauto version, [26](#)
 Oracle Data Guard, [1](#)
 Oracle Enterprise Manager, [2](#)
 log files, [1](#)
 Oracle HTTP Server logs, [19](#)
 Oracle Management Agent
 about log and trace files, [10](#)
 location of log and trace files, [11](#)
 log and trace files, [10](#)
 Oracle Management Repository
 data retention policies, [2](#)
 dropping, [9](#)
 identifying with a connect descriptor, [10](#)
 recreating, [9, 10](#)
 starting the Management Repository
 database, [3](#)
 troubleshooting, [12](#)
 Oracle Management Service
 about the log and trace files, [16](#)
 location the log and trace files, [17](#)
 log and trace files, [16](#)
 Oracle Management Service logs, [17](#)
 Oracle Management Service trace files, [18](#)
 Oracle Process Management and Notification (OPMN)
 using to start and stop the Management Service, [5](#)
 Oracle WebLogic Server logs, [19](#)
 OUI Inventory Configurations, [9](#)
 out-of-box reports, [2](#)

P

Patch Format, [10](#)
 patch management solution
 rolling back patches, [70](#)
 Patches and Updates, [65](#)
 Agent patching
 Add All To Plan, [67](#)
 Create Plan, [67](#)
 Null Platform, [68](#)
 View Plan, [67](#)
 Patches page, [69](#)
 Review and Deploy page, [71](#)
 patching Enterprise Manager
 Management Agent patching errors, [72](#)
 Management Agents
 accessing Patches and Updates, [65](#)
 applying Agent patches, [67](#)
 automated patching, [64](#)
 manual patching, [73](#)
 overview, [63](#)
 searching Patches, [66](#)
 verifying the applied agent patches, [71](#)
 viewing Patch recommendations, [65](#)

patching Enterprise Manager core components, [63](#)

patching Management Agents, [63](#)

patching OMS, [63](#)

patching Repository, [63](#)

performance metrics

- Beacon Aggregation Function
 - maximum value, [14](#)
 - minimum value, [14](#)
 - sum of values, [14](#)
- System Aggregation Function
 - maximum value, [14](#)

Performance Metrics

- Beacon Aggregation Function
 - Average, [14](#)
 - Minimum, [14](#)
 - Sum, [14](#)

personalizing Enterprise Manager pages, [1](#)

plug-in archives, [16](#)

plug-in homes, [30](#)

plug-in id, [12](#)

plug-in manager, [1](#), [8](#), [26](#)

plug-ins, [2](#), [3](#), [10](#), [12](#), [14](#), [15](#), [31](#)

post migration, [31](#)

ProcessManager

- service used to control the Management Service on Windows systems, [5](#)

purge job

- verified, [7](#)

purge policy

- default, [6](#)
- modifying, [6](#)

purging policies, [2](#), [3](#)

- See data retention policies, [2](#)

R

RAID-capable disk

- Management Repository guideline, [1](#)

Reevaluating metric collections, [5](#)

RepManager, [12](#)

Repmanager script, [9](#)

RepManager script, [9](#)

reports

- creating custom reports, [2](#)
- custom, [2](#)
- definitions, Information Publisher, [2](#)
- e-mailing, [4](#)
- generating HTML report, [2](#)
- Information Publisher, [1](#)
- out-of-box, Information Publisher, [2](#)
- predefined report definitions, [2](#)
- report elements, [3](#)
- scheduling, [3](#)
- sharing, [4](#)
- storing and purging, [4](#)

reports (*continued*)

- viewing, [4](#)

retention period, [7](#)

retention times, [5](#)

- default, [5](#)

Root Cause Analysis

- mode
 - automatic, [8](#)
 - manual, [8](#)

S

scheduling

- reports, [3](#)
- reports, flexibility, [3](#)

searching logs, [5](#)

Self Update feature

- setting up, [1](#)
- using, [1](#)

Server Connection Hung

- error while creating the repository, [11](#)

Service Tests and Beacons

- Tests, [10](#)
 - DNS, [10](#)
 - FTP, [10](#)
 - SOAP, [10](#)

Services control panel

- using to start the Management Service, [4](#)

setting your home page, [2](#)

sharing reports, [4](#)

Software Library, [3](#)

- designers, [4](#)
- Operators, [4](#)
- Super Administrators, [4](#)
- users, [4](#)

Software Library Administration, [8](#)

- referenced file locations, [10](#)
 - Agent storage, [11](#)
 - http storage, [10](#)
 - NFS storage, [11](#)
- upload file locations, [9](#)

Software Library console, [1](#)

Software Library referenced locations, [7](#)

Software Library storage, [1](#)

Software library upload locations, [7](#)

Standby OMS System, patching, [27](#)

system patch, [10](#)

T

tables

- modifying retention period, [5](#)

target monitoring credentials

- defined, [7](#)
- setting, [6](#)

trace files

- controlling the contents of Management Service, [18](#)
- controlling the size and number of, [17](#)
- locating Management Agent, [11](#)
- locating Management Service, [17](#)
- Management Agent, [10](#)
- Oracle Management Service, [16](#)

troubleshooting

- general techniques while creating the Management Repository, [12](#)
- Management Service, [28](#)
- while creating the Management Repository, [11](#)

Troubleshooting

- Management Service startup errors, [28](#)

troubleshooting Management Agent, [29](#)

Troubleshooting Management Agent startup errors, [29](#)

U

undeploying plug-ins, [23](#), [25](#)

Universal Installer, [11](#)

updates

- applying in offline mode, [6](#)
- applying in online mode, [5](#)

updating Enterprise Manager, [1](#)

upgrading plug-ins, [21](#), [22](#)

Upgrading Plug-ins, [21](#)

Upgrading Plug-Ins, [21](#)

Usage metrics

- Aggregation Function
- average value, [16](#)
- maximum value, [16](#)
- minimum value, [16](#)
- sum of values, [16](#)

V

verification

- post migration, [28](#)

viewing

- reports, [4](#)

viewing logs, [3](#)