

Oracle® Enterprise Manager

Cloud Control Upgrade Guide

12c Release 1 (12.1.0.1)

E22625-08

May 2012

Oracle Enterprise Manager Cloud Control Upgrade Guide, 12c Release 1 (12.1.0.1)

E22625-08

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

Primary Author: Aravind Jayaraaman

Contributing Author: Namrata Bhakthavatsalam

Contributor: Anu Vale, Smitha Vishwanathan, Abhishek Suresh Kumar, Srilatha Uravakonda, Shachi Sanklecha, Sarun Saseendran, Shilpa Thergaonkar, Palem Naga Maheshwara Reddy, Ranjit Madampath, Maria Teresa Gil Lucientes, Revathy Subburaja, Amitabh Khare, Suman Kumar Pramanik, Sanjay Ediga, Bala Kuchibhotla, Raghu Patti, Magesh Marthandam, Robert Abbott, Raj Aggarwal, Ashwin Karkala, Rahul Goyal, Akanksha Sheoran, Bhavin Desai, David Eschliman, Patrick Combs, Courtney Llamas, Qiang Chen, Laiju Raghuvaran.

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

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

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

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

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

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

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

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

Contents

Preface	ix
Audience	ix
Documentation Accessibility	ix
Related Documents	ix
Conventions	x
Part I Introduction	
1 Overview of Enterprise Manager Cloud Control	
1.1 Overview of Enterprise Manager Cloud Control.....	1-1
1.2 Enterprise Manager Cloud Control Architecture.....	1-2
2 Introduction to Upgrade Approaches	
2.1 Overview of Upgrade Approaches	2-1
2.2 Overview of Upgrade Utilities.....	2-4
2.2.1 Preupgrade Console	2-4
2.2.2 Installation Wizard	2-6
2.2.3 Postupgrade Console	2-7
2.3 Overview of Upgrade Processes.....	2-7
2.3.1 1-System Upgrade Process	2-8
2.3.2 2-System Upgrade Process	2-10
2.3.3 1-System Upgrade Process on a Different Host	2-13
3 Things to Know	
3.1 Supported Upgrade Paths	3-1
3.2 Supported Platforms for Upgrade.....	3-2
3.3 Upgrade Scope	3-2
3.4 Reusing Existing Ports	3-4
3.5 Installing Plug-Ins.....	3-4
3.5.1 Installing Plug-Ins While Upgrading Oracle Management Agent.....	3-4
3.5.2 Installing Plug-Ins While Upgrading Oracle Management Service	3-5
3.6 Discovering and Monitoring Targets.....	3-6
3.7 Managing Notification	3-7
3.8 Managing Alerts.....	3-7

3.8.1	Migrating Alerts.....	3-7
3.8.2	Creating Incidents and Events for Different Types of Open Alerts	3-7
3.8.3	Creating Incidents and Events for Different Types of Closed Alerts.....	3-8
3.9	Managing Jobs	3-8
3.10	Managing Deployment Procedure Runs	3-10
3.11	Using Oracle Software Library	3-10
3.12	Using Connectors.....	3-10
3.13	Collecting Metrics	3-11
3.14	Upgrading EMCLI Clients.....	3-11

Part II Getting Started

4 Upgrading with 1-System Upgrade Approach

5 Upgrading with 2-System Upgrade Approach

6 Upgrading with 1-System Approach on a Different Host

Part III Preupgrade Requirements

7 Configuring Postupgrade Tasks

8 Identifying Host for Enterprise Manager Cloud Control

9 Managing Software

10 Analyzing Your Environment

10.1	Identifying Management Agents with Valid Inventory.....	10-1
10.2	Identifying Management Agents with Invalid Inventory	10-2
10.3	Checking the Upgradability Status of Oracle Management Agents	10-3
10.4	Checking the Upgradability Status of Targets.....	10-4
10.5	Identifying Problematic Oracle Management Agents.....	10-4
10.6	Identifying Management Agents That Need to Be Reconfigured	10-5

Part IV Upgrading Oracle Management Agent

- 11 Deploying and Configuring Oracle Management Agent**
- 12 Generating Health Report of Deployed Oracle Management Agents**
- 13 Verifying and Signing Off the Health Report of Deployed Oracle Management Agents**
- 14 Switching Over to Oracle Management Agent 12c**

Part V Upgrading Oracle Management Service and Oracle Management Repository

15 Providing Repository Backup Details

16 Upgrading OMS and Repository in Graphical Mode

16.1	Upgrading with 1-System Upgrade Approach in Graphical Mode	16-1
16.1.1	Advanced Installer Options	16-7
16.1.2	Limitations	16-8
16.2	Upgrading with 2-System Upgrade Approach in Graphical Mode	16-9

17 Upgrading OMS and Repository in Silent Mode

17.1	Upgrading with 1-System Upgrade Approach in Silent Mode	17-1
17.1.1	Using Advanced Installer Options.....	17-2
17.1.2	Editing Response File for Upgrading with 1-System Upgrade Approach in Silent Mode 17-2	
17.2	Upgrading with 2-System Upgrade Approach in Silent Mode	17-7
17.2.1	Editing Response File for Upgrading with 2-System Upgrade Approach in Silent Mode 17-10	

18 Installing Software Now and Upgrading Later in Graphical Mode

18.1	Upgrading in Software-Only Mode with 1-System Upgrade Approach.....	18-1
18.1.1	Installing Software Binaries	18-1
18.1.2	Running allroot.sh Script.....	18-5
18.1.3	Configuring and Upgrading	18-5
18.2	Upgrading in Software-Only Mode with 2-System Upgrade Approach.....	18-9
18.2.1	Installing Software Binaries	18-9
18.2.2	Running allroot.sh Script.....	18-9
18.2.3	Configuring and Upgrading	18-9

19 Installing Software Now and Upgrading Later in Silent Mode

19.1	Upgrading in Software-Only Mode with 1-System Upgrade Approach.....	19-1
19.1.1	Installing Software Binaries	19-1
19.1.2	After You Install.....	19-4
19.1.3	Configuring and Upgrading	19-4
19.2	Upgrading in Software-Only Mode with 2-System Upgrade Approach.....	19-9

19.2.1	Installing Software Binaries.....	19-9
19.2.2	Running allroot.sh Script.....	19-10
19.2.3	Configuring and Upgrading	19-10

20 Upgrading OMS and Repository for 1-System on Different Host Approach

21 Upgrading Multi-OMS Environment

Part VI Postupgrade Steps

22 Creating Link to Upgraded Oracle Management Repository

23 Reconfiguring Oracle Software Library

24 Checking Agent Upgrade Status

25 Performing General Postupgrade Tasks

25.1	Performing General Postupgrade Steps	25-1
25.2	Stopping OCM Scheduler	25-1
25.3	Deleting Obsolete Targets.....	25-2
25.4	Disabling Incident Rule Sets.....	25-3
25.5	Resolving Metric Collection Errors for SOA Target	25-3
25.6	Enabling Linux Patching After Enterprise Manager Upgrade.....	25-4
25.6.1	Configuring DownloadLatestPackages Job	25-4
25.6.2	Configuring UpdateHostPackages Job	25-4

26 Tracking the Status of Deferred Data Migration Jobs

26.1	Overview of Deferred Data Migration	26-1
26.2	Tracking the Status of Deferred Data Migration Jobs	26-2

27 Tracking the Status of Accrued Data Migration Jobs

27.1	Overview of Accrued Data Migration	27-1
27.2	Tracking the Status of Accrued Data Migration Jobs	27-2

28 Generating and Viewing Diff Reports

28.1	Overview of Diff Reports.....	28-1
28.2	Generating and Viewing Diff Reports	28-1

29 Viewing Inactive Targets in the Upgraded Enterprise Manager System

30 Signing Off Accrued Data Migration Process

31 Updating Incident Rules

31.1	Why Update Incident Rules	31-1
------	---------------------------------	------

31.2	Updating Incident Rules for Moved Metrics	31-3
31.3	Updating Incident Rules for Renamed Metrics	31-4
31.4	Deleting Incident Rules	31-5

Part VII Appendixes

A Overview of Notification in Enterprise Manager Cloud Control

A.1	Understanding Events, Incidents, and Incident Rulesets	A-1
A.2	Accessing Incident Rulesets	A-2
A.3	Migrating Notification Rules to Incident Rulesets	A-3
A.4	Working with Notification Methods and Actions	A-4

B Overview of Metric Changes in Enterprise Manager Cloud Control

B.1	Oracle SOA Infrastructure	B-1
B.2	Oracle SOA Composite	B-1
B.3	Oracle Service Bus	B-2
B.4	Oracle WebLogic Server	B-2
B.5	JBoss Application Server	B-3
B.6	Siebel Enterprise	B-3
B.7	Siebel Server	B-3
B.7.1	Setting Preferred Credentials for Siebel Server	B-4
B.7.2	Setting Preferred Credentials for Siebel Gateway Server	B-4
B.7.3	Setting Preferred Credentials for Siebel Database Repository	B-4

C Identifying Jobs That Will Not Run in the Enterprise Manager System

C.1	Identifying Jobs That Will Not Run in the New, Upgraded Enterprise Manager System	C-1
C.2	Identifying Jobs That Will Not Run in the Existing Enterprise Manager System	C-2

D Meeting Prerequisites for Installing Oracle Management Agent

E Updating Server Load Balancer Configuration Settings

F Setting Preferred Credentials Using EMCLI

G Searching and Adding Oracle Management Agents

H Securing Oracle Management Agents After Backing Up Oracle Management Repository

Index

Preface

Oracle Enterprise Manager Cloud Control Upgrade Guide describes how you can upgrade an existing Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0) or Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0) to Enterprise Manager Cloud Control.

Audience

Oracle Enterprise Manager Cloud Control Upgrade Guide is meant for system administrators who want to upgrade an existing Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0) or Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0) to Enterprise Manager Cloud Control.

Documentation Accessibility

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

Access to Oracle Support

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

Related Documents

For more information, see the following books in the Enterprise Manager Cloud Control documentation library:

- *Oracle Enterprise Manager Cloud Control Basic Installation Guide*
- *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*

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

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

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

Conventions

The following text conventions are used in this document:

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

Part I

Introduction

This part provides an overview of Enterprise Manager Cloud Control, introduces you to the upgrade approaches offered for it, and describes some key facts you must know before you upgrade your Enterprise Manager system.

In particular, this part covers the following:

- [Chapter 1, "Overview of Enterprise Manager Cloud Control"](#)
- [Chapter 2, "Introduction to Upgrade Approaches"](#)
- [Chapter 3, "Things to Know"](#)

Overview of Enterprise Manager Cloud Control

This chapter provides an overview of Oracle Enterprise Manager Cloud Control and helps you understand its architecture and the various core components that are integrated within the product.

This chapter contains the following sections:

- [Overview of Enterprise Manager Cloud Control](#)
- [Enterprise Manager Cloud Control Architecture](#)

1.1 Overview of Enterprise Manager Cloud Control

Enterprise Manager delivers centralized monitoring, administration, and lifecycle management functionality for the complete IT infrastructure, including systems running Oracle and non-Oracle technologies.

Your environment may comprise multiple Oracle Databases, Oracle WebLogic Servers, Web applications deployed on these servers, hosts running these targets, and so on. You can, of course, use the individual product consoles to monitor the status of each of these targets, but it becomes cumbersome to shuttle between multiple console windows and track the performance of each of these targets using so many windows.

Enterprise Manager Cloud Control offers a solution that allows you to monitor and manage the complete Oracle IT infrastructure from a single console. In addition, it provides support for business-driven IT management and business-centric top-down application management to manage your business services, user experience, and infrastructure. It also offers support for monitoring certain non-Oracle products, for example, IBM WebSphere Application Server, Microsoft SQL Server, Juniper Networks NetScreen Firewall, and so on.

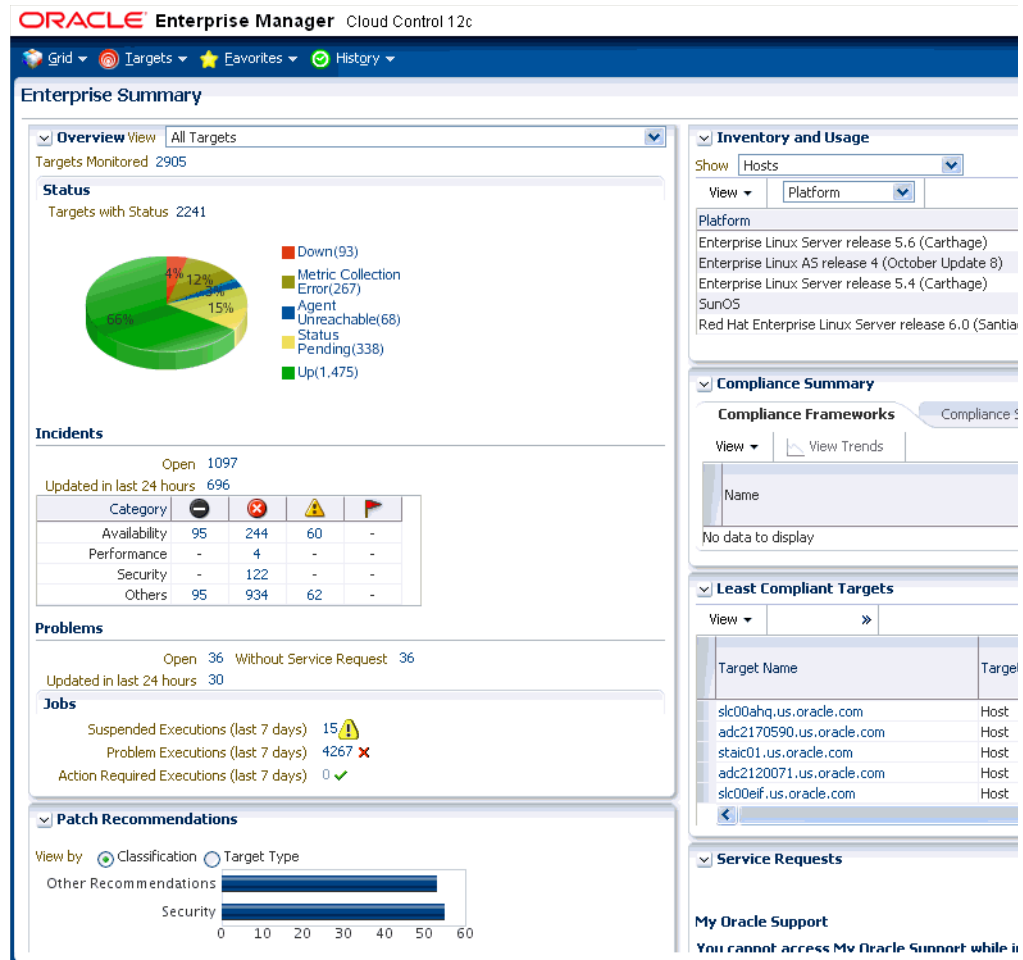
Note: Enterprise Manager Cloud Control does not require a private or public cloud.

Enterprise Manager has had many releases in the past, but Enterprise Manager Cloud Control is the latest release that has significant changes over all its earlier releases. Unlike the earlier releases that were called Enterprise Manager *Grid* Control, this release is called Enterprise Manager *Cloud* Control.

Enterprise Manager Cloud Control offers a variety of new features and enhancements, including improved user interface, stability, reliability, and performance. In addition, Enterprise Manager Cloud Control offers seamless access to *My Oracle Support* from

within its console for managing service requests, deploying patches, and reviewing knowledge base articles.

Figure 1–1 Enterprise Manager Cloud Control Console



With a broad set of end-to-end monitoring, administration, configuration management, provisioning, and security capabilities, Enterprise Manager Cloud Control reduces the cost and complexity of managing computing environments. Robust service-level management functionality within Enterprise Manager Cloud Control dramatically improves service levels through rich transaction and end-user performance monitoring and deep diagnostics for multi-tier Internet applications.

For more information about Enterprise Manager Cloud Control, access the following URL:

<http://www.oracle.com/us/products/enterprise-manager/index.html>

1.2 Enterprise Manager Cloud Control Architecture

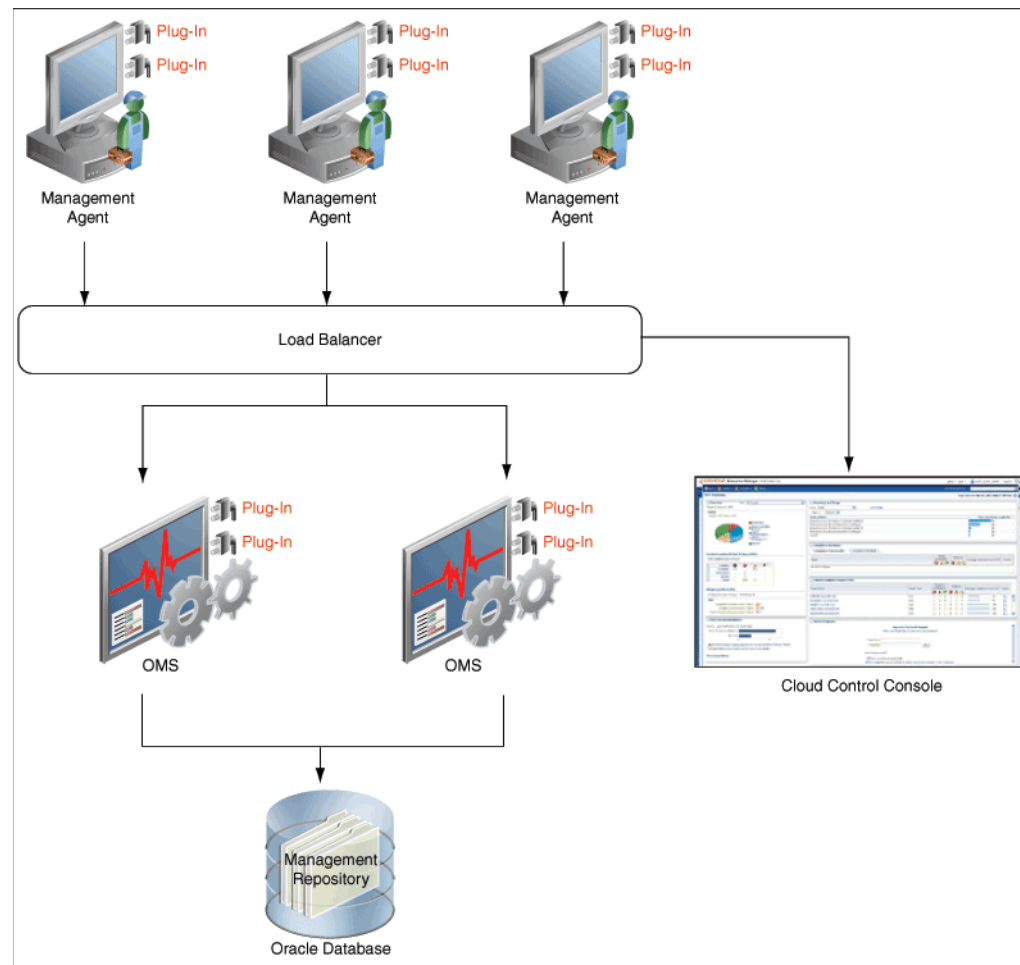
Enterprise Manager Cloud Control includes the following components:

- Oracle Management Agent
- Oracle Management Service

- Oracle Management Repository
- Oracle Management Plug-Ins
- Enterprise Manager Cloud Control Console

Figure 1–2 shows a sample Enterprise Manager Cloud Control architecture and illustrates how these core components fit into the architecture.

Figure 1–2 Enterprise Manager Cloud Control Architecture



Note: In Figure 1–2, the load balancer and the multiple OMSes are depicted only to indicate how a sample Enterprise Manager Cloud Control architecture would look in a large organization. They are not a prerequisite or a requirement for an Enterprise Manager system installation in a small enterprise. If you do not have a load balancer, then the Management Agents communicate directly with the OMSes.

For information about sizing your Enterprise Manager deployment and identifying when you need a load balancer, refer to the *Oracle Enterprise Manager Cloud Control Administrator's Guide*.

The following sections describe the core components of Enterprise Manager Cloud Control.

Oracle Management Agent (Management Agent)

The Management Agent is an integral software component that enables you to convert an unmanaged host to a managed host in the Enterprise Manager system. The Management Agent works in conjunction with the plug-ins to monitor the targets running on that managed host.

Oracle Management Service (OMS)

The OMS is a Web-based application that orchestrates with the Management Agents and the Management Plug-Ins to discover targets, monitor and manage them, and store the collected information in a repository for future reference and analysis. The OMS also renders the user interface for the Enterprise Manager Cloud Control console. The OMS is deployed to the Oracle Middleware Home (middleware home), which is the parent directory that has the Oracle WebLogic Server home, the OMS home, the Management Agent home, the plug-in home, the Java Development Kit (JDK), the OMS instance base directory, the Oracle WT directory, the Oracle Common directory, and other relevant configuration files and directories. While deploying the OMS, the Enterprise Manager Cloud Control Installation Wizard installs Oracle WebLogic Server if it does not already exist in your environment. As a result, a WebLogic Server admin console is also installed.

Oracle Management Repository (Management Repository)

The Management Repository is a storage location where all the information collected by the Management Agent gets stored. It consists of objects such as database jobs, packages, procedures, views, and tablespaces.

The OMS uploads the monitoring data it receives from the Management Agents to the Management Repository. The Management Repository then organizes the data so that it can be retrieved by the OMS and displayed in the Enterprise Manager Cloud Control console. Since data is stored in the Management Repository, it can be shared between any number of administrators accessing the Enterprise Manager Cloud Control.

At the time of installation, the Enterprise Manager Cloud Control Installation Wizard configures the Management Repository in your existing, certified database. The wizard, however, does not install a new database.

Oracle Management Plug-Ins (Plug-Ins)

Plug-Ins are pluggable entities that offer special management capabilities customized to suit specific target types. Unlike the earlier releases of Enterprise Manager, in Enterprise Manager Cloud Control, the plug-ins work in conjunction with the OMS and the Management Agent to monitor every target in your environment. Therefore, they are deployed to the OMS as well as the Management Agent. In the earlier releases, plug-ins enabled you to monitor only third-party targets, but in Enterprise Manager Cloud Control, plug-ins enable you to monitor all types of targets in your environment.

Plug-ins have independent release cycles, so every time you have a new version of an Oracle product released, you will have a new version of the plug-in released to support monitoring of that new product version in Enterprise Manager Cloud Control. This simplifies things because you no longer have to wait to upgrade your Enterprise Manager system to support a new product version; instead you can upgrade your plug-ins to monitor the new product version.

[Table 1–1](#) lists the mandatory plug-ins that are installed by default with Enterprise Manager Cloud Control. In addition to these mandatory plug-ins, you can optionally install other plug-ins available in the software kit (DVD, downloaded software, and so

on). The installer offers a screen where you can select the optional plug-ins and install them.

Table 1–1 Mandatory Plug-Ins Installed with Enterprise Manager Cloud Control

Name	Description
Oracle Database	Enables you to monitor and manage Oracle Database and related targets such as Oracle Real Application Clusters (Oracle RAC), Oracle Automatic Storage Management (Oracle ASM), and so on.
Oracle Fusion Middleware	Enables you to monitor and manage Oracle Fusion Middleware products such as Oracle WebLogic Domain, Oracle WebLogic AdminServer, Oracle WebLogic Server, Oracle SOA Suite, Oracle Web Tier, and so on.
Oracle My Oracle Support	Enables you to log in to My Oracle Support from within the Cloud Control console, search the knowledge library for notes and documents, raise service requests, and create patch plans and templates for patching monitored targets.
Oracle Exadata	Enables you to monitor and manage Oracle Exadata targets.

Enterprise Manager Cloud Control Console

The Enterprise Manager Cloud Control console is the user interface you see after you install Enterprise Manager Cloud Control. With the help of the console, you can monitor and administer your entire computing environment from one location on the network. All the systems and services including enterprise application systems, databases, hosts, middleware application servers, listeners, and so on, are easily managed from one central location.

Introduction to Upgrade Approaches

With the option of deploying Enterprise Manager across the enterprise and in any number of permutations, upgrading the entire environment becomes a very complex activity involving updating of software and configurations in different levels (tiers) located in different hosts. In addition, there are challenges of upgrading the environment with *near-zero* downtime or minimal monitoring loss.

Considering these challenges, Oracle offers upgrade options that not only offer the flexibility to select the approach that best suits your requirement but also aim at simplifying the entire upgrade operation with the intent of making it seamless and error-free.

This chapter provides an overview of these upgrade approaches. In particular, this chapter covers the following:

- [Overview of Upgrade Approaches](#)
- [Overview of Upgrade Utilities](#)
- [Overview of Upgrade Processes](#)

2.1 Overview of Upgrade Approaches

Oracle offers the following upgrade approaches to upgrade your existing Enterprise Manager system:

- **1-System Upgrade Approach:** This approach enables you to upgrade to Enterprise Manager Cloud Control on the same host where your earlier release of Enterprise Manager is running. This approach also upgrades the Oracle Management Repository (Management Repository) in the existing database. Since the upgrade happens on the same host, there is a reasonable downtime involved.

This approach does not refer to upgrading of an Enterprise Manager system in an environment with one Oracle Management Service (OMS). It refers to upgrading of an Enterprise Manager system on the same host as the old one, and having only one Enterprise Manager system existing at any point. To learn about upgrading a multi-OMS environment, see [Chapter 21](#).

- **2-System Upgrade Approach:** This approach enables you to install Enterprise Manager Cloud Control on a host that is different from the host where your existing Enterprise Manager system is running.

This approach does not upgrade the Management Repository in the existing database, but upgrades the one in the backed up database, thus enabling two Enterprise Manager systems to exist. Since a new Enterprise Manager system coexists with the old one, there is *no* or *near zero* downtime involved.

- 1-System Upgrade Approach on a Different Host:** This approach enables you to install Enterprise Manager Cloud Control on a host different from where the existing Enterprise Manager is running.

This approach is similar to the 2-System upgrade approach, but unlike the 2-System upgrade approach, this approach upgrades the Management Repository in the existing database itself. Since only one Enterprise Manager system exists at any point, there is a reasonable downtime involved.

Table 2–1 lists the differences between the three upgrade approaches:

Table 2–1 Differences Between the Upgrade Approaches

1-System Upgrade Approach	2-System Upgrade Approach	1-System Upgrade Approach on Different Host
Involves predeployment and switch over of Management Agents prior to upgrading the OMS and the Management Repository, unlike the traditional approach that focussed on upgrading only the OMS and the Management Repository.	Resembles fresh installation.	Resembles fresh installation.
Requires a reasonable downtime. <i>(Essentially, the downtime lasts from the time you switch over the Management Agents till the time you upgrade the OMS.)</i>	Requires minimum or zero downtime.	Requires a reasonable downtime.
Upgrades to Enterprise Manager Cloud Control on the same host where your earlier release of Enterprise Manager is running.	Installs Enterprise Manager Cloud Control on a host that is different from the host where your existing Enterprise Manager system is running.	Installs Enterprise Manager Cloud Control on a host different from where the existing Enterprise Manager is running, but upgrades the Management Repository in the existing database itself.
Does not require an additional hardware resource because it upgrades on the same host.	Requires an additional hardware resource because it installs on a different host.	Requires an additional hardware resource because it installs on a different host.
Existing Enterprise Manager system must be shut down so that the configuration information can be copied and carried over to the upgraded Enterprise Manager system.	Existing Enterprise Manager system can continue to run until you switch over all your earlier releases of Management Agents to the newly upgraded environment.	Existing Enterprise Manager system must be shut down so that the configuration information can be copied and carried over to the new system.
Management Agents must be deployed and configured <i>before</i> upgrading the OMS and the Management Repository.	Management Agents can be deployed and configured <i>before</i> or <i>after</i> upgrading the OMS and the Management Repository.	Management Agents must be deployed and configured <i>before</i> upgrading the OMS and the Management Repository.
Management Agents can be deployed and configured in an incremental or phased manner, that is, in groups.	Management Agents can be deployed and configured in an incremental or phased manner, that is, in groups.	Management Agents can be deployed in an incremental or phased manner, that is, in groups.

Table 2–1 (Cont.) Differences Between the Upgrade Approaches

1-System Upgrade Approach	2-System Upgrade Approach	1-System Upgrade Approach on Different Host
Management Agents must be switched over <i>before</i> upgrading the OMS and the Management Repository.	Management Agents must be switched over <i>after</i> upgrading the OMS and the Management Repository.	Management Agents must be switched over <i>before</i> upgrading the OMS and the Management Repository.
Upgrades the Management Repository in the existing, certified database.	Upgrades the Management Repository in the backed up database. Therefore, as a prerequisite, you are required to back up your existing Oracle Database.	Upgrades the Management Repository in the existing, certified database.
Requires no changes to the ports and firewall settings. The upgraded Management Agents and the OMS use the same ports used earlier.	Requires some changes to the ports and firewall settings. The upgraded Management Agents use the same ports used earlier. However, the Management Agent and the OMS installed on the remote host might use new ports. In a multi-OMS environment, if you have a Server Load Balancer (SLB), then you can either open up new ports for the new Management Agent and the OMS in the same SLB, or configure a completely new SLB for them.	Requires some changes to the ports and firewall settings. The upgraded Management Agents use the same ports used earlier. However, the Management Agent and the OMS installed on the remote host might use new ports. In a multi-OMS environment, if you have a Server Load Balancer (SLB), then you can either open up new ports for the new Management Agent and the OMS in the same SLB, or configure a completely new SLB for them.
All deployment procedures must be finished before the upgrade is started. Otherwise, the scheduled procedures will be canceled, and you will have to re-create them.	All deployment procedures must be finished before the upgrade is started. Otherwise, the scheduled procedures will be canceled, and you will have to re-create them.	All deployment procedures must be finished before the upgrade is started. Otherwise, the scheduled procedures will be canceled, and you will have to re-create them.
Running jobs will be aborted at the start of the downtime.	Running jobs will continue to run on the existing Enterprise Manager system after the start of the backup. In Enterprise Manager Cloud Control, these jobs will appear to be aborted or failed.	Running jobs will be aborted at the start of the downtime.
Scheduled jobs will run after the downtime is over if their grace period allows them. Otherwise, they will be skipped.	Scheduled jobs will run on the existing Enterprise Manager system from the time of the backup until the point where the Management Agent for that target is migrated to Enterprise Manager Cloud Control. Once the Management Agent is migrated, the jobs will run in Enterprise Manager Cloud Control.	Scheduled jobs will run after the downtime is over if their grace period allows them. Otherwise, they will be skipped.

Table 2–1 (Cont.) Differences Between the Upgrade Approaches

1-System Upgrade Approach	2-System Upgrade Approach	1-System Upgrade Approach on Different Host
Repeating jobs will run at their next scheduled time after the downtime. If repeating jobs fall within the downtime, they may be skipped.	Repeating jobs will continue to run according to their schedule on the existing Enterprise Manager system. Once the Management Agent is migrated, subsequent runs will be in Enterprise Manager Cloud Control.	Repeating jobs will run at their next scheduled time after the downtime. If repeating jobs fall within the downtime, they may be skipped.

Note: Jobs run either in the existing Enterprise Manager system or in Enterprise Manager Cloud Control, and not on both systems. The true status of a job must be viewed only on the system where it actually ran. For more information, see [Appendix C](#). Also, job executions with multiple targets will not run on either system unless all Management Agents for all targets are migrated at the same time.

2.2 Overview of Upgrade Utilities

To enable you to select one of the upgrade approaches, orchestrate the entire upgrade operation seamlessly, and also track the post-upgrade activities such as the data migration processes, Oracle offers the following utilities:

- [Preupgrade Console](#)
- [Installation Wizard](#)
- [Postupgrade Console](#)

2.2.1 Preupgrade Console

The *Enterprise Manager 12c Upgrade Console* acts as the primary user interface and is indeed the starting point for upgrading your Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0) or Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0) to Enterprise Manager Cloud Control.

The *Enterprise Manager 12c Upgrade Console* enables you to select an appropriate upgrade approach, predeploy the Oracle Management Agent 12c software, and switch over the earlier releases of Management Agents to the newly predeployed Management Agents.

Note: Oracle Management Service 12c communicates only with Oracle Management Agent 12c. Therefore, unlike the earlier releases, you must first upgrade the Management Agents in your system before upgrading your existing OMS. Hence, the *Enterprise Manager 12c Upgrade Console* acts as a starting point to the upgrade process.

To access the *Enterprise Manager 12c Upgrade Console*, apply the preupgrade console patch on your existing Enterprise Manager system. For information about the patch you need to download and apply for your platform, access the following URL:

<http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html>

After downloading the patch, follow the instructions outlined in the ReadMe, which is packaged with the patch. Ensure that you use the latest release of OPatch to apply the patch. After applying the patch, log in with super administrator privileges to access the *Enterprise Manager 12c Upgrade Console*.

IMPORTANT:

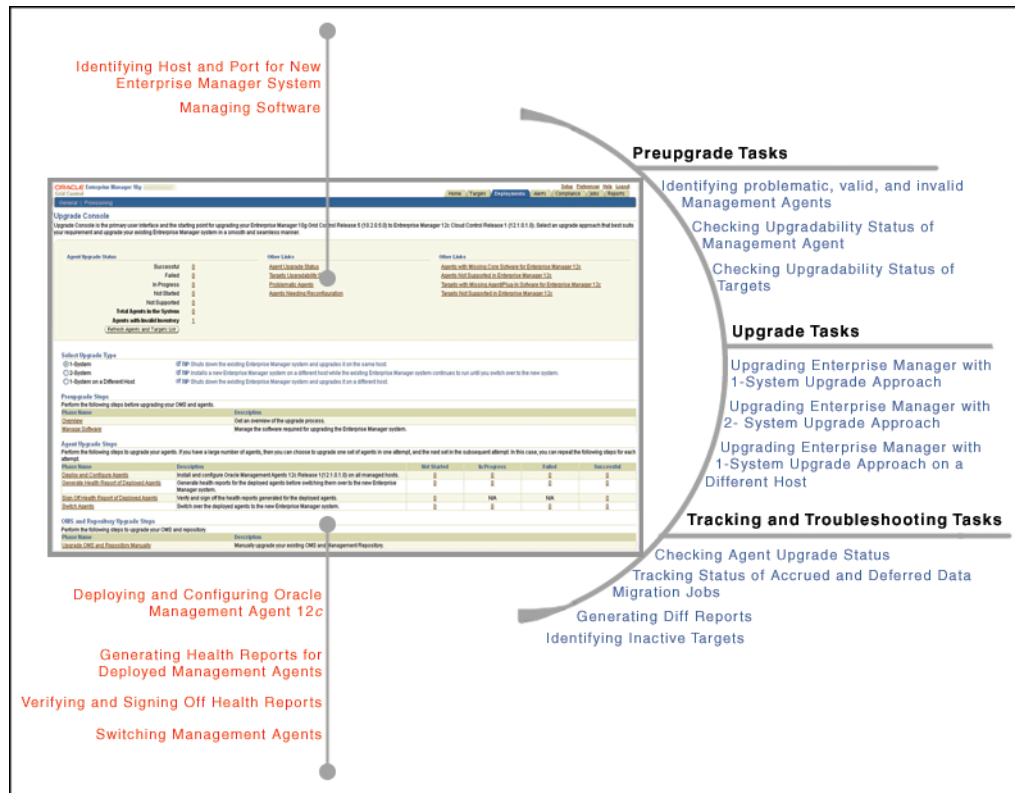
- You will have to shut down your OMS to apply the patch, and as a result, your Enterprise Manager system will be down until you complete the patching operation.
 - Despite applying the patch, if you do not see the hyperlink to the *Enterprise Manager 12c Upgrade Console* on the Deployments page, then do the following:
 1. Move the `jsp_servlet` directory out of the following location:

```
$<OMS_INSTANCE_BASE>/user_user_projects/domains/GCDomain/generated_classes
```
 2. Stop the OMS from the OMS home:

```
$<OMS_HOME>/bin/emctl stop oms
```
 3. Restart the OMS from the OMS home:

```
$<OMS_HOME>/bin/emctl start oms
```
-
-

The following diagram clearly illustrates the features it offers.

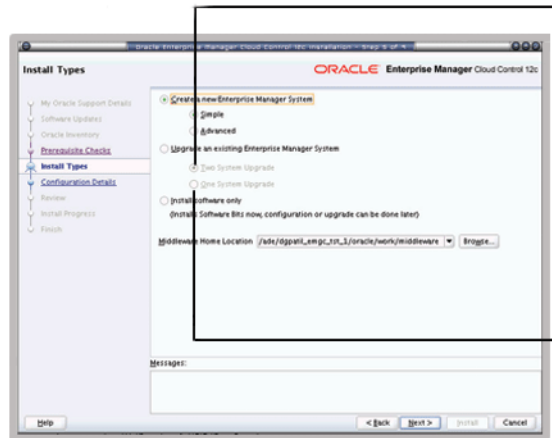


Note: The supported earlier releases for upgrade include: Oracle Management Agent 10g Release 2 (10.2.x.x.x), Oracle Management Agent 11g Release 1 (11.1.0.1.0), Oracle Management Service 10g Release 5 (10.2.0.5.0), and Oracle Management Service 11g Release 1 (11.1.0.1.0).

2.2.2 Installation Wizard

The Enterprise Manager Cloud Control Installation Wizard is the primary user interface that enables you to select the type of upgrade approach you want to perform, and upgrade your existing OMS and Management Repository.

The following diagram clearly illustrates the features it offers.



Two System Upgrade Approach

Installs and configures Enterprise Manager Cloud Control on the host, and while this happens, the existing Enterprise Manager system continues to run until you switch over all your earlier releases of Oracle Management Agents to the newly upgraded environment. You can choose to switch over the Oracle Management Agents in an incremental or phased manner, so that minimum or zero downtime is experienced. This way, you have a highly available environment.

One System Upgrade Approach

Upgrades your existing Enterprise Manager system to Enterprise Manager Cloud Control, and while this happens, the existing Enterprise Manager system remains shut down so that the configuration information can be copied and carried over to the new system.

2.2.3 Postupgrade Console

The Postupgrade Console is the primary user interface for tracking all post-upgrade activities, including accrued data migration jobs and deferred data migration jobs. In addition, you can generate diff reports and view a list of targets that are currently inactive in the upgraded Enterprise Manager system.

The following diagram clearly illustrates the features it offers.

Deferred Data Migration Jobs

Tracks the post-upgrade activity that migrates the format of the data stored in the existing Enterprise Manager system to the format compatible with Enterprise Manager Cloud Control.

Accrued Data Migration Jobs

Tracks the post-upgrade activity that migrates the accrued data stored in the old Management Repository to the upgraded Management Repository.

Diff Reports

Provides information about the configuration or setup-related changes that were manually made to the earlier release of Enterprise Manager while it was being upgraded

Targets with Pending Activation

Provides a list of targets that are inactive in Enterprise Manager Cloud Control.

Sign Off

Enables you to sign off the Accrued Data Migration Process for each of the Management Agents.

Note: For more information about these jobs, refer to [Chapter 26](#), [Chapter 27](#), [Chapter 28](#), and [Chapter 29](#).

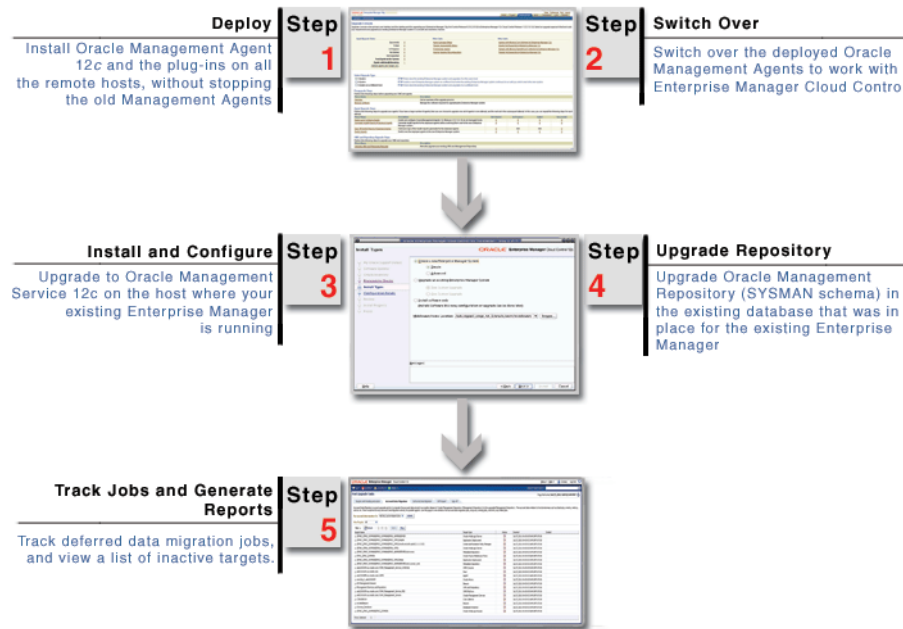
2.3 Overview of Upgrade Processes

This section describes the high-level flow or sequence of steps to be followed for each of the upgrade approaches. In particular, this section describes the following:

- 1-System Upgrade Process
- 2-System Upgrade Process
- 1-System Upgrade Process on a Different Host

2.3.1 1-System Upgrade Process

The following illustration describes the high-level flow or sequence of steps you must perform when you choose to upgrade using the 1-System upgrade approach:



Using the *Enterprise Manager 12c Upgrade Console*, you can deploy the Oracle Management Agent 12c software and switch over the old Management Agents to the newly deployed Management Agents. You will notice that *Deploy* and *Switch Over* are two different operations, although they deal with installing and upgrading Management Agents.

Note: As a best practice, Oracle recommends you to complete the *Deploy* operation well before you start the *Switch Over* operation.

While the *Deploy* operation involves copying of software binaries of the Management Agent and configuring them on the hosts, the *Switch Over* operation involves stopping the old Management Agents and starting the new Management Agents to work with Enterprise Manager Cloud Control.

The two operations are separated and treated as different entities to ensure that your existing Enterprise Manager system is not shut down or disturbed in any way while the software binaries are copied and configured on the hosts. Once the software binaries are copied and configured, you can switch them over with much less time because the time taken is only for stopping the old Management Agents and starting the new Management Agents.

Once you have switched over the Management Agents, you can upgrade the OMS and the Management Repository.

Note: As a best practice, Oracle also recommends you to upgrade the OMS immediately after you complete the *Switch Over* operation. Note that the downtime in 1-System upgrade approach essentially lasts from the time you switch over the Management Agent till the time you upgrade your OMS. So the more you delay your upgrade operation, the more the downtime. During this downtime, none of the targets are monitored and no monitoring data is uploaded to the OMS.

When you upgrade to Enterprise Manager Cloud Control on the host using the installation wizard, the installation wizard does the following by default:

- Upgrades your OMS and Management Agent
- Installs Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24 (JDK). Also installs Oracle JRF 11g Release (11.1.1.4.0), which includes the `oracle_common` directory, and Oracle Web Tier 11g Release (11.1.1.4.0), which includes the `Oracle_WT` directory.

Note: Oracle WebLogic Server 11g Release 1 (10.3.5) and JDK 1.6 v24 are installed only if they do not exist in your environment. If they already exist (supported version or higher version), then the installer detects them and displays the middleware home where they are installed. In this case, you only need to validate the path to this middleware home.

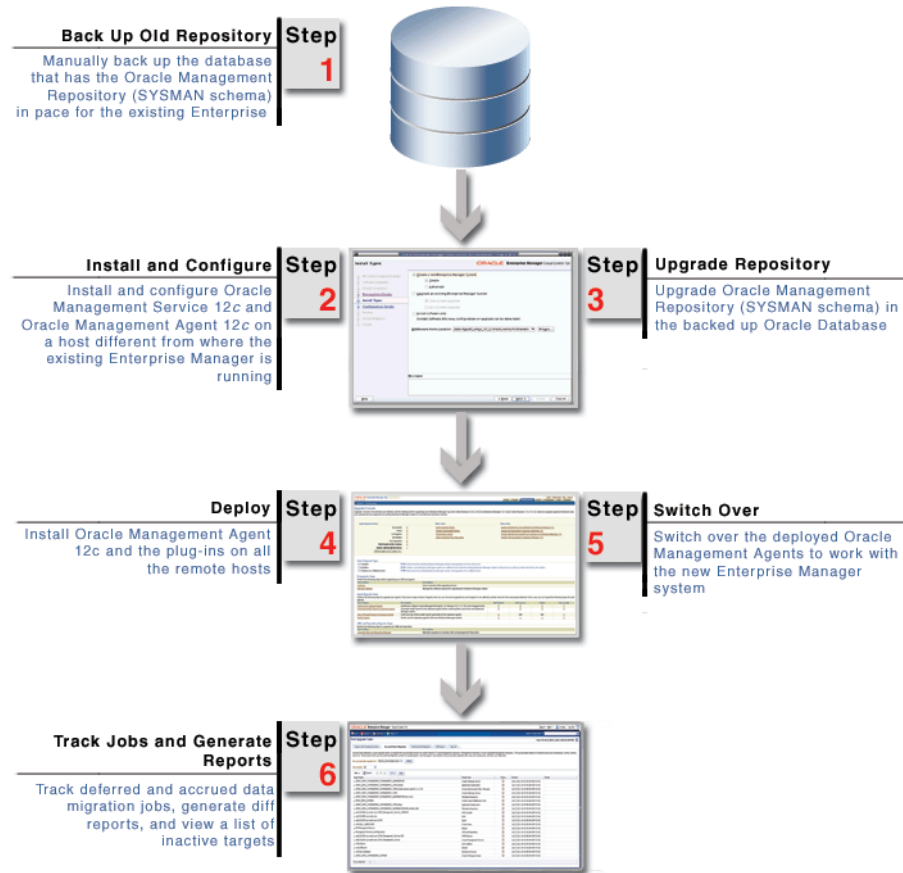
- Installs the following plug-ins:
 - Oracle Database Management Plug-In
 - Oracle Fusion Middleware Management Plug-In
 - Oracle My Oracle Support Management Plug-In
 - Oracle Exadata Management Plug-In
 - Other plug-ins you installed while predeploying Oracle Management Agent 12c using the *Enterprise Manager 12c Upgrade Console* (that is, if these plug-ins are available in the software kit)
- Creates or reuses the Oracle WebLogic domain, the Admin Server, the Node Manager, and the Managed Server, depending on the earlier release of the Enterprise Manager system from which you are upgrading.
 - If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0), then by default, the following are created:
 - * An Oracle WebLogic domain called `GCDomain` is automatically created during the configuration of Enterprise Manager Cloud Control. For this WebLogic Domain, a default user account, `weblogic`, is used as the administrative user. You can choose to change this, if you want, in the installer.
 - * A Node Manager user account called `nodemanager` is automatically created during the configuration of Enterprise Manager Cloud Control. A Node Manager enables you to start, shut down, or restart an Oracle WebLogic Server instance remotely, and is recommended for applications with high availability requirements.

- If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0), then the same Oracle WebLogic domain and Node Manager, which were created for your earlier Enterprise Manager system, will be reused for the new system.
- Creates the OMS instance base directory (`gc_inst`) in the middleware home you enter in the wizard, and stores all configuration information related to the OMS.
- Runs the following configuration assistants to configure the installed or upgraded components:
 - Plugins Prerequisites Check
 - Repository Upgrade Assistant
 - MDS Schema Configuration Assistant
 - OMS Configuration Assistant
 - Plugins Deployment and Configuration Assistant
 - Start Oracle Management Service
 - Plugins Inventory Migration
 - Oracle Configuration Manager Repeater Configuration Assistant
 - Oracle Configuration Manager for OMS

Note: The installer does NOT upgrade your existing Management Agent because it is predeployed by the *Enterprise Manager 12c Upgrade Console*.

2.3.2 2-System Upgrade Process

The following illustration describes the high-level flow or sequence of steps you must perform when you choose to upgrade using the 2-System upgrade approach:



When you install and configure Enterprise Manager Cloud Control on the target host using the installer, the installer does the following by default:

- Installs the following components in the middleware home location you enter in the installation wizard:
 - Java Development Kit (JDK) 1.6 v24
 - Oracle WebLogic Server 11g Release 1 (10.3.5)
 - Oracle Management Service 12c
 - Oracle Management Agent 12c
 - Oracle JRF 11g Release (11.1.1.4.0), which includes `oracle_common` directory
 - Oracle Web Tier 11g Release (11.1.1.4.0), which includes `Oracle_WT` directory
 - Oracle Management Plug-Ins
 - * Oracle Database Management Plug-In
 - * Oracle Fusion Middleware Management Plug-In
 - * Oracle My Oracle Support Management Plug-In
 - * Oracle Exadata Management Plug-In
 - * Other plug-ins you installed while predeploying Oracle Management Agent 12c using the *Enterprise Manager 12c Upgrade Console* (that is, if these plug-ins are available in the software kit)

Note: Oracle WebLogic Server 11g Release 1 (10.3.5) and JDK 1.6 v24 are installed only if they do not exist in your environment. If they already exist (supported version or higher version), then the installer detects them and displays the middleware home where they are installed. In this case, you only need to validate the path to this middleware home.

- Creates an Oracle WebLogic domain called `GCDomain`. For this WebLogic Domain, a default user account, `weblogic`, is used as the administrative user. You can choose to change this, if you want, in the installer.
- Creates a Node Manager user account called `nodemanager`. A Node Manager enables you to start, shut down, or restart an Oracle WebLogic Server instance remotely, and is recommended for applications with high availability requirements.
- Configures an OMS Instance Base location in the middleware home, for storing all configuration details related to Oracle Management Service 12c. 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/Middleware/gc_inst`. You can choose to change this, if you want, in the installer.

- Runs the following configuration assistants to configure the installed or upgraded components:
 - Plugins Prerequisites Check
 - Repository Upgrade Assistant
 - MDS Schema Configuration
 - OMS Configuration
 - Plugins Deployment and Configuration
 - Start Oracle Management Service
 - Plugins Inventory Migration
 - Oracle Configuration Manager Repeater Configuration
 - Oracle Configuration Manager for OMS
 - Agent Configuration Assistant
- Secures the OMS by generating a password internally. This password is generated by the OMS Configuration Assistant, and the password expires in 30 days from the time it is generated.

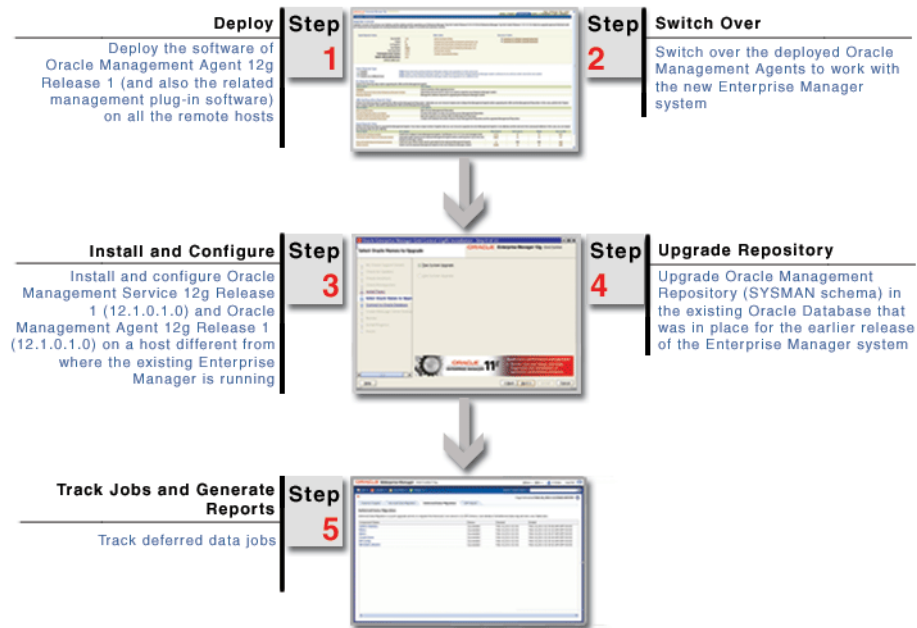
If the OMS Configuration Assistant or the Plugins Deployment and Configuration Assistant fails, then ensure that you resolve the issue within the 30-day period. Otherwise, you will face an error in securing the Management Agent while running the Agent Configuration Assistant.

If you are unable to resolve the issue within the 30-day period, run the following command from the Management Agent home:

```
$(AGENT_HOME)/sysman/install/agentDeploy.sh OMS_HOST=<oms_host_name> EM_UPLOAD_PORT=<oms_upload_https_port> AGENT_REGISTRATION_PASSWORD=<agent_reg_password>
```

2.3.3 1-System Upgrade Process on a Different Host

The following illustration describes the high-level flow or sequence of steps you must perform when you choose to upgrade using the 1-System upgrade approach on a different host:



As you can see in the illustration, this approach is a combination of 1-System upgrade approach and 2-System upgrade approach. Much like 1-System upgrade approach, you start the upgrade process by predeploying and switching over the Management Agents. Then, like the 2-System upgrade approach, you install Enterprise Manager Cloud Control on a remote host. However, the difference is, you upgrade the same Management Repository that you have been using for the earlier release of the Enterprise Manager, and then decommission the earlier release. This way, only one Enterprise Manager system exists at a given time.

You install the software binaries of Enterprise Manager Cloud Control on the remote host, then upgrade the existing Management Repository, and then, configure the software binaries to complete the installation.

While installing the software binaries, you create Oracle homes and install the following components in the middleware home location:

- Java Development Kit (JDK) 1.6 v24
- Oracle WebLogic Server 11g Release 1 (10.3.5)
- Oracle Management Service 12c
- Oracle Management Agent 12c
- Oracle JRF 11g Release (11.1.1.4.0), which includes `oracle_common` directory
- Oracle Web Tier 11g Release (11.1.1.4.0), which includes `Oracle_WT` directory
- Oracle Management Plug-Ins
 - Oracle Database Management Plug-In
 - Oracle Fusion Middleware Management Plug-In

- Oracle My Oracle Support Management Plug-In
- Oracle Exadata Management Plug-In

While configuring the software binaries, you do the following:

- Create an Oracle WebLogic domain called `GCDomain`. For this WebLogic Domain, a default user account, `weblogic`, is used as the administrative user. You can choose to change this, if you want, in the installer.
- Create a Node Manager user account called `nodemanager`. A Node Manager enables you to start, shut down, or restart an Oracle WebLogic Server instance remotely, and is recommended for applications with high availability requirements.
- Configure an Oracle Management Service Instance Base location (`gc_inst`) in the middleware home, for storing all configuration details related to Oracle Management Service 12c.

For example, if the middleware home is `/u01/app/Oracle/Middleware/`, then the instance base location is `/u01/app/Oracle/Middleware/gc_inst`.

- Configures the plug-ins and the Management Agent.

Things to Know

Before you use the upgrade approaches to upgrade to Enterprise Manager Cloud Control, keep these points in mind:

- [Supported Upgrade Paths](#)
- [Supported Platforms for Upgrade](#)
- [Upgrade Scope](#)
- [Reusing Existing Ports](#)
- [Installing Plug-Ins](#)
- [Discovering and Monitoring Targets](#)
- [Managing Notification](#)
- [Managing Alerts](#)
- [Managing Jobs](#)
- [Managing Deployment Procedure Runs](#)
- [Using Oracle Software Library](#)
- [Collecting Metrics](#)
- [Using Connectors](#)
- [Upgrading EMCLI Clients](#)

3.1 Supported Upgrade Paths

The following upgrade paths are supported:

- You can upgrade from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0) directly to Enterprise Manager Cloud Control
- You can upgrade from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0) directly to Enterprise Manager Cloud Control.
- You can upgrade from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0) to Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0), and then upgrade to Enterprise Manager Cloud Control.

If you have Enterprise Manager 10g Grid Control Release 1 (10.1) or Enterprise Manager 10g Grid Control Release 4 (10.2.0.4.0) or lower, then you must first upgrade or patch them to Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0) or Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0). After upgrading or

patching them to the supported releases, upgrade them to Enterprise Manager Cloud Control.

3.2 Supported Platforms for Upgrade

The following platforms are supported:

- 1-System upgrade, understandably, must always be done on the same platform as the earlier release of the Enterprise Manager system because you are upgrading on the same host.
- 2-System upgrade is possible on the same platform as the earlier release of the Enterprise Manager system, and from Linux (32-bit) to Linux (64-bit) (or vice versa) because you are upgrading on a remote host.
- 1-System upgrade on a different host is possible on the same platform as the earlier release of the Enterprise Manager system, and from Linux (32-bit) to Linux (64-bit) (or vice versa) because you are upgrading on a remote host, much like 2-System upgrade approach.

3.3 Upgrade Scope

The following are some facts about the upgrade approaches:

- You can choose to use either 1-System, 2-System, or 1-System upgrade approach on a different host. However, regardless of the approach you choose, the upgrade operation is always an out-of-place upgrade where you see new Oracle homes of Oracle Management Service (OMS) and Oracle Management Agent (Management Agent).
- The upgrade approaches do NOT upgrade your existing database where the Management Repository is configured.

To upgrade such databases, use the database upgrade tool. For more information, on the upgrade tool, see the *Oracle Database Upgrade Guide* available in the Oracle Database documentation library at:

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

- Oracle Management Service 12c communicates only with Oracle Management Agent 12c. Therefore, it is important to upgrade your Management Agents before upgrading your OMS.
- You can upgrade any Management Agent as long as the Oracle Management Agent 12c software for that platform is available.
- You must not upgrade to Enterprise Manager Cloud Control in a middleware home that is on an NFS-mounted drive. Upgrading on an NFS-mounted drive causes the Oracle HTTP Server to restart frequently, which in turn makes the OMS inaccessible. If you are forced to upgrade on such a shared drive, then ensure that the OMS instance base directory (`gc_inst`) is created in a non-NFS-mounted location.
- The Enterprise Manager Cloud Control Installation Wizard installs Java Development Kit (JDK) 1.6 v24 and Oracle WebLogic Server 11g Release 1 (10.3.5) if they do not exist in your environment.
- If Oracle WebLogic Server 11g Release 1 (10.3.5) does not exist, then Oracle recommends you to allow the installation wizard to install it for you. However, if

you want to manually install it, then ensure that you install it using JDK 1.6 v24+ (64-bit version for 64-bit platforms and 32-bit version for 32-bit platforms).

- Download JDK 1.6 v24+ for your platform from the platform vendor's Web site. For example, download SUN JDK 1.6 v24+ for Linux platforms from Oracle Web site. Similarly, download the JDK for other platforms from other vendors' trusted Web sites.
- If you already have JDK, then verify its version by navigating to the <JDK_Location>/bin directory and running the following command:

```
./java -fullversion"
```

To verify whether it is a 32-bit or a 64-bit JDK, run the following command:

```
"file *"
```

- JROCKIT is not supported.
- If you want to manually install Oracle WebLogic Server 11g Release 1 (10.3.5) on Linux 64-bit platforms, first install the 64-bit JDK for your platform, and then download and use the `wls1035_generic.jar` file to install Oracle WebLogic Server.

For example,

```
<JDK home>/bin/java -d64 -jar <absolute_path_to_wls1035_generic.jar>
```

- If you want to manually install Oracle WebLogic Server 11g Release 1 (10.3.5) on Linux 32-bit platforms, then download and use either the `wls1035_linux32.bin` file or the `wls1035_generic.jar` file.

For example,

```
<JDK home>/bin/java -jar <absolute_path_to_wls1035_generic.jar>
```

- You must follow the instructions outlined in the *Oracle® Fusion Middleware Installation Guide for Oracle WebLogic Server* to install Oracle WebLogic Server. The guide is available in the Fusion Middleware documentation library available at:

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

- You must ensure that the Oracle WebLogic Server installation is a typical installation, and even if you choose to perform a custom installation, ensure that components chosen for custom installation are the same as the ones associated with a typical installation.
- You must ensure that the user installing the WebLogic Server is the same as the one installing Enterprise Manager Cloud Control.

- You must ensure that the Oracle WebLogic Server 11g Release 1 (10.3.5) installed by the Enterprise Manager Cloud Control Installation Wizard or by you is dedicated for Enterprise Manager Cloud Control. You must not have any other Oracle Fusion Middleware product installed in that middleware home.

Enterprise Manager Cloud Control cannot coexist with any Oracle Fusion Middleware product in the same middleware home because the `ORACLE_COMMON` property is used by both the products.

3.4 Reusing Existing Ports

When you upgrade your Management Agents, the ports used by the earlier release of the Management Agents are carried over to the upgraded Management Agents. Therefore, your firewall settings are not affected in any way.

When you upgrade your OMS, the following ports are assigned:

- For 2-System upgrade approach, the Enterprise Manager Cloud Control Installation Wizard assigns default ports to all the core components.

For information about the core components, the range within which a port is selected, and the free port that is assigned, see the chapter on installation basics in the *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.

- For 1-System upgrade approach, the ports used for the earlier release of the following core components are carried over:
 - Enterprise Manager Upload HTTP Port
 - Enterprise Manager Upload HTTP SSL Port
 - Enterprise Manager Central Console HTTP Port
 - Enterprise Manager Central Console HTTP SSL Port
 - Oracle Management Agent

However, for the rest of the core components, the Enterprise Manager Cloud Control Installation Wizard assigns default ports, unless other values are provided in the wizard.

For information about the core components, the range within which a port is selected, and the free port that is assigned, see the chapter on installation basics in the *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.

3.5 Installing Plug-Ins

To identify the plug-ins required for upgrade, in the *Enterprise Manager 12c Upgrade Console*, in the Preupgrade Steps section, click **Manage Software**. On the Manage Software page, view the plug-ins that are required for upgrading your system.

The plug-ins listed on the Manage Software page are based on the targets monitored by the old Management Agents in your existing system, and also based on the new plug-in requirement Enterprise Manager Cloud Control has. You need all the plug-ins listed on this page to successfully upgrade your existing system.

This section describes how you can download and install the required plug-ins while upgrading the Management Agent and OMS. In particular, this section covers the following:

- [Installing Plug-Ins While Upgrading Oracle Management Agent](#)
- [Installing Plug-Ins While Upgrading Oracle Management Service](#)

3.5.1 Installing Plug-Ins While Upgrading Oracle Management Agent

To install the required plug-ins while upgrading the Management Agents, follow these steps:

1. Access the following URL:

<http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html>

2. Download the Management Agent software to an accessible location. Do NOT extract the contents of the software ZIP file. The Management Agent software is platform-specific, so ensure that you copy the software for the platform on which you want to install.
3. Download all the required plug-ins to the same location. Plug-ins are generic, so they are common for all platforms.

Ensure that you download all the plug-ins listed as required plug-ins on the Manage page, whether or not you want to monitor a target with them. You may feel that a few plug-ins are not required because you do not have targets to be monitored by them, but those plug-ins may be required for upgrading your system. Therefore, download all the plug-ins listed on the Manage Software page. Ensure that you download these plug-ins before backing up the database that contains the Management Repository.

Note: You can also download these plug-ins from the <software_kit>/plugins directory, but Oracle recommends you to download them from OTN so that you always procure the latest plug-ins and the plug-ins for all platforms.

Note: To identify what plug-ins are required, in the *Enterprise Manager 12c Upgrade Console*, in the Preupgrade Steps section, from the table, click **Manage Software**. On the Manage Software page, in the Plug-In Software section, see the required plug-ins.

Download all the plug-ins listed as required plug-ins on the Manage Software page, whether or not you want to monitor a target with them. You may feel that a few plug-ins are not required because you do not have targets to be monitored by them, but those plug-ins may be required for upgrading your system. Therefore, download all the plug-ins listed on the Manage Software page. And ensure that you download these plug-ins before backing up the database that contains the Management Repository.

4. In the *Enterprise Manager 12c Upgrade Console*, on the Manage Software page (Preupgrade Steps section), in the Provide Software Location section, enter the absolute path to the directory where the plug-in is present, and click **Validate** to register that location with the Management Repository.

See: For information about registering and validating the plug-in location, see [Chapter 9](#).

3.5.2 Installing Plug-Ins While Upgrading Oracle Management Service

To install the required plug-ins while upgrading the OMS, invoke the installer and proceed to the Select Plug-Ins screen. The screen lists all the required plug-ins you registered via the the *Enterprise Manager 12c Upgrade Console* while upgrading the Management Agents. The mandatory ones are enabled by default.

Note: If you had missed registering some required plug-ins, then the wizard prompts you to visit the *Enterprise Manager 12c Upgrade Console* to register them before proceeding with the upgrade.

Ensure that the software for the plug-ins listed on this screen are available in the Enterprise Manager Cloud Control software kit (DVD or downloaded software). If the software for the required plug-ins are not available, then do the following:

- Manually download the plug-ins from the following URL to an accessible location:
<http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html>
- Invoke the installation wizard and pass the plug-in download location:

```
./runInstaller -pluginLocation <absolute_path_to_plugin_software_location>
```

3.6 Discovering and Monitoring Targets

After you upgrade a Management Agent, by default, the Management Agent and the host on which you upgraded the Management Agent get automatically discovered in the Enterprise Manager Cloud Control console.

After you upgrade an OMS, by default, the following get automatically discovered in the Enterprise Manager Cloud Control console:

- Oracle WebLogic Domain (for example, GCDomain)
- Oracle WebLogic AdminServer
- Oracle WebLogic Server
- Oracle Web Tier
- Application deployments, one for the Enterprise Manager Cloud Control console and one for the platform background services.
- Oracle Management Service
- Oracle Management Repository
- Oracle Management Agent
- The host on which you upgraded the OMS

However, the other targets running on that host and other hosts do not get automatically discovered and monitored. To monitor the other targets, you need to add them to Enterprise Manager Cloud Control either using the Auto Discovery Results page, the Add Targets Manually page, or the discovery wizards offered for the targets you want to monitor.

For information about discovering targets in Enterprise Manager Cloud Control, refer to the *Oracle Enterprise Manager Cloud Control Administrator's Guide* available in the Enterprise Manager documentation library at:

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

3.7 Managing Notification

After upgrading the entire Enterprise Manager system, all notification rules and alerts created in the earlier release continue to work in Enterprise Manager Cloud Control. However, note that they have been enhanced and subsumed into a larger and newer concept—*Notification Rules* are now called *Incident Rulesets*, and *Alerts* are now called *Events* in Enterprise Manager Cloud Control.

For information about *Incident Rulesets* and how they map to notification rules, and for information about *Events* and how they map to alerts, see [Appendix A](#).

3.8 Managing Alerts

During upgrade, the alerts from the earlier release are migrated as *Events* in Enterprise Manager Cloud Control in the following manner. For 1-System upgrade approach, the alerts are migrated while upgrading the Management Repository. For 2-System upgrade approach, the alerts are migrated while backing up the Management Repository to the remote host.

This section covers the following:

- [Migrating Alerts](#)
- [Creating Incidents and Events for Different Types of Open Alerts](#)
- [Creating Incidents and Events for Different Types of Closed Alerts](#)

3.8.1 Migrating Alerts

The following are the ways in which the alerts are migrated:

- All open alerts are migrated.
[Table 3–1](#) shows how and when incidents and events are created for different types of open alerts.
- All alerts that were closed 180 days prior to upgrading or backing up the Management Repository are migrated as part of the Deferred Data Migration Process. This period of 180 days can be changed by the administrator.
[Table 3–2](#) shows how and when incidents and events are created for different types of closed alerts. Also note that if a closed alert had an associated ticket, then that information is not captured as part of the event migration.
- All open statefull alerts, and open stateless alerts created within 7 days prior to upgrading or backing up the Management Repository are migrated.

Note: In case of 2-System upgrade approach, if an alert is created in the earlier release of the Enterprise Manager system after the Management Repository is backed up, then that open alert is migrated as part of the Accrued Data Migration Process (see [Table 3–1](#)). In addition, all availability records are also migrated as part of the Accrued Data Migration Process.

3.8.2 Creating Incidents and Events for Different Types of Open Alerts

[Table 3–1](#) shows how and when incidents and events are created for different types of open alerts.

Table 3–1 Incidents and Events Created for Different Types of Open Alerts

Open Alert Type	Incident Created	Event Created
Critical Alert	Yes	Yes
Warning Alert	No	Yes
Critical Alert with Ticket	Yes	Yes (with Ticket)
Warning Alert with Ticket	Yes	Yes (with Ticket)
Warning Alert with Notification Pending	Yes	Yes
Warning Alert without Notification Pending	No	Yes
Critical Alert with Acknowledgement	Yes	Yes
Warning Alert with Acknowledgement	Yes	Yes

3.8.3 Creating Incidents and Events for Different Types of Closed Alerts

Table 3–2 shows how and when incidents and events are created for different types of closed alerts. Also note that if a closed alert had an associated ticket, then that information is not captured as part of the event migration.

Table 3–2 Incidents and Events Created for Different Types of Closed Alerts

Closed Alert Type	Incident Created	Event Created
Critical Alert	No	Yes
Warning Alert	No	Yes
Critical Alert with Ticket	No	Yes (without Ticket)
Warning Alert with Ticket	No	Yes (without Ticket)
Warning Alert with Notification Pending	No	Yes
Warning Alert without Notification Pending	No	Yes
Critical Alert with Acknowledgement	No	Yes
Warning Alert with Acknowledgement	No	Yes

3.9 Managing Jobs

For 1-System upgrade approach, jobs can run more or less as expected. During the downtime, jobs do not run, and any job that is running during the downtime is aborted or failed. In addition, all the scheduled jobs continue as they were planned.

For 2-System upgrade approach, there are some restrictions and caveats on how jobs run. Firstly, since a Management Agent is monitored only by one particular Enterprise Manager system at any point, jobs can run only in the system that monitors the Management Agent. Until a Management Agent is migrated, all jobs against targets monitored by that Management Agent are run in the old Enterprise Manager system. This also means that only one Enterprise Manager system has the *true* status of a job because the Management Agent communicates only with one of the systems at a given time, so only that Enterprise Manager system knows what the actual status is.

- If a Management Agent is not migrated, then a future job appears as a scheduled job in the old Enterprise Manager system, but appears as a suspended job on the Management Agent unavailable in Enterprise Manager Cloud Control.
- A job running in the old Enterprise Manager system at the time of the backup either aborts or fails in Enterprise Manager Cloud Control. Once the Management

Agent is migrated, a future job appears as a suspended job on the Management Agent unavailable in the old Enterprise Manager system, but appears as a scheduled job in Enterprise Manager Cloud Control. If the Management Agent is subsequently removed from the old Enterprise Manager system, then that job is removed as well.

If the backup of the old Enterprise Manager system did not require a downtime, then the jobs running at the time of the backup continue to run. (If the backup required a downtime, then the job may abort due to the downtime.) Such jobs appear as aborted, failed, or skipped jobs in Enterprise Manager Cloud Control.

- Repeating jobs continue to run in the old Enterprise Manager system according to their schedule. In Enterprise Manager Cloud Control, such jobs appear to be aborted, failed, or skipped. Once the Management Agent is migrated, such jobs start to run in Enterprise Manager Cloud Control. In the old Enterprise Manager system, such jobs are suspended on the Management Agent unavailable.
- Jobs submitted in the old Enterprise Manager system after the backup do NOT appear in Enterprise Manager Cloud Control. Jobs submitted in Enterprise Manager Cloud Control do NOT appear in the old Enterprise Manager system. Usually, jobs are created only in the system that is currently monitoring the target.
 - Jobs created in the old Enterprise Manager system before the Management Agent of its targets is migrated run in the old Enterprise Manager system as expected.
 - Repeating jobs run until the Management Agent is migrated at which point they are stuck as suspended jobs on the Management Agent unavailable.
 - If jobs are created in the old Enterprise Manager system after the target is migrated, then they never run; they remain stuck as suspended jobs on the Management Agent unavailable. So do not create a job in the old Enterprise Manager system after the Management Agent is migrated.
 - Jobs created in Enterprise Manager Cloud Control on targets for which the Management Agent has already been migrated behave normally and run as expected.
 - Jobs can be created in Enterprise Manager Cloud Control before the Management Agent for its target is migrated, but they will be in suspended mode on Management Agent unavailable until the Management Agent is migrated.

This is particularly useful when a new job is created in the old Enterprise Manager system and a copy of it is desired in Enterprise Manager Cloud Control for use after the target is migrated. Usually, this will be a repeating job.

- * If the Management Agent is migrated before the scheduled time of the job, then the job runs in Enterprise Manager Cloud Control.
- * If the Management Agent is migrated after the scheduled time of the job, then the job is skipped. This is to prevent a case where the job runs on both the systems.
- * If the job has a repeating schedule, then the times before the migration are skipped, while the times after the migration are run.
- * A job with an immediate schedule does not run in Enterprise Manager Cloud Control and is eventually skipped. So do not create an immediate job on target that is not migrated.

- For jobs with multiple executions, one job per target, some targets may be suspended, while others run.

Consider a job against two databases, *dbA* monitored by Management Agent *A*, and *dbB* monitored by Management Agent *B*. If only Management Agent *B* is migrated, then the execution for *dbA* is suspended, while the execution for *dbB* runs when it reaches its scheduled time. If this is a repeating job, then the execution for *dbA* is skipped. Once the Management Agent *A* is migrated, then both executions are run as usual.

This behavior is important for jobs with many targets, such as those submitted to a group. Those executions for targets monitored by the old Enterprise Manager system run in the old Enterprise Manager system, while those for targets monitored by Enterprise Manager Cloud Control run in Enterprise Manager Cloud Control. The corresponding executions on the other systems are suspended or skipped.

- For jobs on multiple targets, one job for many targets, the jobs can neither run in the old Enterprise Manager system nor in Enterprise Manager Cloud Control unless the Management Agents for all the targets are migrated at one time. To determine the correct set of Management Agents to migrate at one time to address this, run the SQL queries described in [Appendix C](#).

The alternative is to migrate the Management Agents independently, and then, once the last Management Agent is migrated, the job may run if the grace period allows it to run or if the scheduled time was after the last agent migration.

3.10 Managing Deployment Procedure Runs

After upgrading the entire Enterprise Manager system, none of the old deployment procedure runs will be available in the upgraded Enterprise Manager. If you want to reference any of the old runtime data, then you must use the following EM CLI verb to export all of the runtime data as an XML file.

```
get_instance_data_xml
```

3.11 Using Oracle Software Library

The following is the status of Oracle Software Library (Software Library) after the Enterprise Manager is upgraded:

- For 1-System upgrade approach, the Software Library is functional the moment the Enterprise Manager is upgraded. No manual effort is required to make it functional.
- For 2-System upgrade approach, the Software Library is functional only when it is reconfigured after the Enterprise Manager is upgraded.

To understand the 2-System upgrade approach workflow and to know when you must reconfigure the Software Library, see [Chapter 5](#). For information about reconfiguring the Software Library, see [Chapter 23](#).

- For 1-System upgrade approach on a different host, the Software Library is functional the moment the Enterprise Manager is upgraded.

3.12 Using Connectors

After upgrading the entire Enterprise Manager system, the connectors that were configured with your old Enterprise Manager system will continue to work in

Enterprise Manager Cloud Control. However, the ones that were not configured will not work.

3.13 Collecting Metrics

Some metrics related to the Oracle Fusion Middleware targets have been renamed in Enterprise Manager Cloud Control. In addition, a few have been introduced. The following are the targets for which the metrics have undergone some changes. For information about the metric changes, see [Appendix B](#).

- Oracle SOA Infrastructure
- Oracle SOA Composite
- Oracle Service Bus
- Oracle WebLogic Server
- JBoss Application Server
- Siebel Enterprise
- Siebel Server

In general, do not modify the metric thresholds after deploying and configuring the Management Agents.

3.14 Upgrading EMCLI Clients

You must upgrade all *existing* EMCLI clients of the earlier release to 12c Release 1 so that they can work with Enterprise Manager Cloud Control. This means, you must discard the old one and set up a new one.

For information about setting up a new EMCLI client, see the *Enterprise Manager Command Line Interface Download* page within the Cloud Control console. To access that page, in Cloud Control, from the **Setup** menu, select **My Preferences**, and then, click **Command Line Interface**.

Part II

Getting Started

This part describes the high-level process you must follow for each of the upgrade approaches. Oracle strongly recommends you to read the chapters covered in this part, and consider this part to be the starting point for upgrading your existing Enterprise Manager system.

This part covers the following chapters:

- [Chapter 4, "Upgrading with 1-System Upgrade Approach"](#)
- [Chapter 5, "Upgrading with 2-System Upgrade Approach"](#)
- [Chapter 6, "Upgrading with 1-System Approach on a Different Host"](#)

Upgrading with 1-System Upgrade Approach

To upgrade your existing Enterprise Manager system to Enterprise Manager Cloud Control with 1-System upgrade approach, follow these steps:

Table 4–1 Upgrading Enterprise Manager with 1-System Upgrade Approach

Step No.	Step	Procedure
Step 1	Prepare Yourself	
(a)	Learn about the 1-System upgrade approach.	Chapter 2
(b)	Review the important facts you need to know before you begin.	Chapter 3
Step 2	Perform Preupgrade Tasks	
(a)	Apply the preupgrade console patch on your existing Enterprise Manager system to get access to the <i>Enterprise Manager 12c Upgrade Console</i> .	Section 2.2.1
(b)	Manually download the following software, and stage them to an accessible location: <ul style="list-style-type: none"> ▪ Oracle Management Agent 12c ▪ All the required plug-ins 	Section 3.5.1
(c)	Provide information about the location of the software you manually downloaded and staged in Step 2 (b)	Chapter 9
(d)	Analyze your environment to identify Oracle Management Agents (Management Agent) with valid and invalid inventory, check their upgradability status, and identify the problematic Management Agents. If a required software is missing, then repeat Step (b) and Step (c).	Chapter 10
(e)	Meet the prerequisites for upgrading the Management Agents.	Appendix D
Step 3	Upgrade Oracle Management Agent	
(a)	Deploy and configure the software binaries of Oracle Management Agent 12c.	Chapter 11
(b)	Generate a health report and check the readiness of the predeployed Management Agents.	Chapter 12
(c)	Verify and sign off the health check report.	Chapter 13

Table 4–1 (Cont.) Upgrading Enterprise Manager with 1-System Upgrade Approach

Step No.	Step	Procedure
(d)	<p>Switch over the old Management Agents to the newly deployed ones so that they can communicate with Enterprise Manager Cloud Control.</p> <p><i>Note: If you have a large number of agents, then you can choose to upgrade one set of Oracle Management Agents in one attempt, and the next set in the subsequent attempt. In this case, you can repeat Step 3 (a) to Step 3 (d) for each attempt.</i></p>	Chapter 14
(e)	If you have a Server Load Balancer (SLB) configured, then modify the settings of your monitors.	Appendix E
Step 4	Upgrade Oracle Management Service and Oracle Management Repository	
(a)	<p>On the host where your existing Enterprise Manager is running, meet the following prerequisites:</p> <ul style="list-style-type: none"> ■ Meet the Oracle Management Service-related prerequisites described in the chapter on installing Enterprise Manager Cloud Control, in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>. ■ Meet the Management Agent-related prerequisites described in Appendix D. ■ Meet the following Power Broker and SUDO setup requirements: <p>If you have Power Broker set up, then disable the welcome message.</p> <p>If you have SUDO set up, then ensure that you have SUDO privileges to invoke <code>/bin/sh</code> as <code>root</code>. Ensure that you have the line <code>Defaults visiblepw</code> in the <code>/etc/sudoers</code> file. Also ensure that you comment out the line <code>Defaults requiretty</code> in the file.</p> 	

Table 4–1 (Cont.) Upgrading Enterprise Manager with 1-System Upgrade Approach

Step No.	Step	Procedure
(b)	<p>On the Management Repository, meet the following prerequisites:</p> <ul style="list-style-type: none"> ■ Ensure that the MGMT_CONNECTOR_CONFIG table does not have any NULL rows. To verify this, run the following SQL query. <pre>select * from mgmt_cntr_config where connector_type_guid IS NULL and connector_guid IS null;</pre> <p>Typically, the command must not return any rows. If it does return any rows, then run the following SQL query to clean the table:</p> <pre>delete from mgmt_cntr_config where connector_guid IS NULL or connector_type_guid IS NULL; commit;</pre> ■ Ensure that there are no custom-created materialized views in the Management Repository. To verify this, run the following SQL query. Typically, the command must not return any rows. If it does return any rows, then contact Oracle Support. <pre>select count(1) from ALL_MVIEW_LOGS where log_owner=<EM_REPOS_USER></pre> ■ Ensure that the tables do not have any snapshots created. To verify this, log in to the Management Repository and run the following SQL query as SYSMAN user: <pre>select master , log_table from all_mview_logs where log_owner='<EM_REPOS_USER></pre> <p>For example,</p> <pre>select master , log_table from all_mview_logs where log_owner='SYSMAN'</pre> <p>If there are snapshots created in a table, then the query displays the master table and the snapshot details. For example,</p> <pre>SQL> master log_table em-violations em\$violation_log</pre> <p>If there are snapshots, then drop them by running the following command as SYSMAN user:</p> <pre>SQL> Drop snapshot log on <master></pre> <p>For example,</p> <pre>SQL> Drop snapshot log on em-violations</pre> 	
(c)	<p>Stop all running and scheduled deployment procedures in your existing Enterprise Manager system before upgrading the system.</p>	

Table 4–1 (Cont.) Upgrading Enterprise Manager with 1-System Upgrade Approach

Step No.	Step	Procedure
(d)	<p><i>(Only if you have Application Dependency and Performance (ADP) or JVM Diagnostics (JVMD) installed)</i></p> <ol style="list-style-type: none"> 1. Take an inventory of the JVMs and WebLogic Domains being monitored by JVMD and/or ADP. 2. Deinstall the JVMD and ADP applications from your inventory by logging into the WebLogic Administration Console for each monitored domain and removing the <i>jamagent</i> and <i>Acsera</i> application deployments. 3. Shut down all of your ADP and JVMD managers. 4. Remove all ADP and JVMD managed servers from the GCDomain using the WebLogic Administration Console. 5. Run purge scripts for JVMD: <ol style="list-style-type: none"> (a) Navigate to the following location: <code><middleware_home>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.1.0/archives/jvmd/</code> (b) Extract the file <code>jvmd.zip</code>. (c) Run the script <code>jvmd_monitoringupgrade11_12.sql</code>. (d) Run the script <code>jvmd_traceupgrade11_12.sql</code> if there are existing Thread Snapshots from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1). 	
(e)	<p>Copy the emkey from the OMS to the Management Repository:</p> <ul style="list-style-type: none"> ■ If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5), then run the following command from the OMS home: <code>\$<OMS_HOME>/bin/emctl config emkey -copy_to_repos -sysman_pwd <sysman_pwd></code> ■ If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), then run the following command from the OMS home: <code>\$<OMS_HOME>/bin/emctl config emkey -copy_to_repos_from_file -repos_host <repository_host> -repos_port <port> -repos_sid <sid> -repos_user <username> [-repos_pwd <pwd>] [-admin_pwd <pwd>] -emkey_file <OMS_HOME>/sysman/config/emkey.ora</code> 	
(f)	<p>Stop the OMS you are about to upgrade and also the other OMSes that connect to it.</p>	
(g)	<p>Upgrade the OMS and the Management Repository. You can choose to upgrade in graphical or silent mode. You can also choose to install the software binaries at one point and upgrade them later in graphical or silent mode.</p>	<p>Chapter 16, Chapter 17, Chapter 18, or Chapter 19</p>
Step 5	Perform Postupgrade Task	
(a)	Perform the general post-upgrade tasks.	Chapter 25
(b)	Track the status of deferred data migration jobs.	Chapter 26
(c)	Update the incident rules for metrics associated with the OMS.	Chapter 31

Table 4–1 (Cont.) Upgrading Enterprise Manager with 1-System Upgrade Approach

Step No.	Step	Procedure
(e)	<p data-bbox="586 258 1243 317"><i>(Only if you have Application Dependency and Performance (ADP) or JVM Diagnostics (JVMD) installed)</i></p> <ol style="list-style-type: none"> <li data-bbox="586 327 1208 464">1. If you have not deinstalled the JVMD and ADP applications from your inventory by logging into the WebLogic Administration Console for each monitored domain and removing the <i>jamagent</i> and <i>Acsera</i> application deployments, then do so now. <li data-bbox="586 474 1235 716">2. Delete all <i>ad4jTarget</i> targets: <ol style="list-style-type: none"> <li data-bbox="634 516 1036 541">(a) Navigate to the following location: <middleware_home>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.1.0/archives/jvmd/ <li data-bbox="634 642 948 667">(b) Extract the file <i>jvmd.zip</i>. <li data-bbox="634 684 1219 709">(c) Run the script <i>jvmd_targetupgrade11_12.sql</i>. <li data-bbox="586 726 1235 968">3. Delete all <i>OCAMM Manager</i> targets: <ol style="list-style-type: none"> <li data-bbox="634 768 1235 884">(a) Navigate to the following location: <middleware_home>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.1.0/archives/ocamm/ <li data-bbox="634 900 1036 926">(b) Extract the file <i>ADPManager.zip</i>. <li data-bbox="634 942 1198 968">(c) Run the script <i>adp_targetupgrade11_12.sql</i>. <li data-bbox="586 978 1053 1003">4. Deploy new JVMD and ADP managers. <li data-bbox="586 1020 1170 1073">5. Deploy new JVMD and ADP agents based on your inventory. 	

Upgrading with 2-System Upgrade Approach

To upgrade your existing Enterprise Manager system to Enterprise Manager Cloud Control with 2-System upgrade approach, follow these steps:

Table 5–1 Upgrading Enterprise Manager with 2-System Upgrade Approach

Step No.	Step	Procedure
Step 1	Prepare Yourself	
(a)	Learn about the 2-System upgrade approach.	Chapter 2
(b)	Review the important facts you need to know before you begin.	Chapter 3
Step 2	Perform Preupgrade Tasks	
(a)	Apply the preupgrade console patch on your existing Enterprise Manager system to get access to the <i>Enterprise Manager 12c Upgrade Console</i> .	Section 2.2.1
(b)	Provide information about the host where you plan to upgrade your existing OMS.	Chapter 8
(c)	Manually download the following software, and stage them to an accessible location: <ul style="list-style-type: none"> ▪ Oracle Management Agent 12c ▪ All the required plug-ins 	Section 3.5.1
(d)	Provide information about the location of the software you manually downloaded and staged in Step 2 (c)	Chapter 9
(e)	Analyze your environment to identify Oracle Management Agents (Management Agent) with valid and invalid inventory, check their upgradability status, and identify the problematic Management Agents. If a required software is missing, then repeat Step (c) and Step (d).	Chapter 10
(f)	Meet the prerequisites for upgrading the Management Agents.	Appendix D
Step 3	Upgrade Oracle Management Service and Oracle Management Repository <i>Note: Optionally, you can choose to deploy and configure your Oracle Management Agents before upgrading the Oracle Management Service and Oracle Management Repository. In this case, perform Step 4 (a) before Step 3 (a) to Step 3 (l).</i>	

Table 5–1 (Cont.) Upgrading Enterprise Manager with 2-System Upgrade Approach

Step No.	Step	Procedure
(a)	<p>On the remote host where you plan to install Enterprise Manager Cloud Control, meet the following prerequisites:</p> <ul style="list-style-type: none"> ■ Meet the Oracle Management Service-related prerequisites described in the chapter on installing Enterprise Manager Cloud Control, in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>. ■ Meet the Management Agent-related prerequisites described in Appendix D. ■ Meet these additional requirements: <p>If you have Power Broker set up, then disable the welcome message.</p> <p>If you have SUDO set up, then ensure that you have SUDO privileges to invoke <code>/bin/sh</code> as <code>root</code>. Ensure that you have the line <code>Defaults visibletpw</code> in the <code>/etc/sudoers</code> file. Also ensure that you comment out the line <code>Defaults requiretty</code> in the file.</p> 	
(b)	<p>Stop all running and scheduled deployment procedures in your existing Enterprise Manager system before upgrading the system.</p>	
(c)	<p><i>(Only if you have Application Dependency and Performance (ADP) or JVM Diagnostics (JVMD) installed)</i></p> <ol style="list-style-type: none"> 1. Take an inventory of the JVMs and WebLogic Domains being monitored by JVMD and/or ADP. 2. Deinstall the JVMD and ADP applications from your inventory by logging into the WebLogic Administration Console for each monitored domain and removing the <i>jamagent</i> and <i>Acsera</i> application deployments. 3. Shut down all of your ADP and JVMD managers. 4. Remove all ADP and JVMD managed servers from the GCDomain using the WebLogic Administration Console. 5. Run purge scripts for JVMD: <ol style="list-style-type: none"> (a) Navigate to the following location: <pre><middleware_home>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.1.0/archives/jvmd/</pre> (b) Extract the file <code>jvmd.zip</code>. (c) Run the script <code>jvmd_monitoringupgrade11_12.sql</code>. (d) Run the script <code>jvmd_traceupgrade11_12.sql</code> if there are existing Thread Snapshots from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1). 	

Table 5–1 (Cont.) Upgrading Enterprise Manager with 2-System Upgrade Approach

Step No.	Step	Procedure
(d)	<p>Copy the emkey from the OMS to the Management Repository:</p> <ul style="list-style-type: none"> ■ If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5), then run the following command from the OMS home: <pre data-bbox="634 422 1224 474">\$<OMS_HOME>/bin/emctl config emkey -copy_to_repos -sysman_pwd <sysman_pwd></pre> ■ If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), then run the following command from the OMS home: <pre data-bbox="634 579 1224 762">\$<OMS_HOME>/bin/emctl config emkey -copy_to_repos_from_file -repos_host <repository_host> -repos_port <port> -repos_sid <sid> -repos_user <username> [-repos_pwd <pwd>] [-admin_pwd <pwd>] -emkey_file <OMS_HOME>/sysman/config/emkey.ora</pre> 	
(e)	<p><i>(Only if your old Enterprise Manager system has Oracle Software Library configured)</i></p> <p>If you have Oracle Software Library (Software Library) configured, then back up each of the configured Software Library directories to a location accessible from the remote host where you plan to install Enterprise Manager Cloud Control.</p> <p>The location to which you back up the directories is required for reconfiguring the Software Library [as described in Step 3 (l)] once you install Enterprise Manager Cloud Control.</p> <p>For example, if your Software Library was configured in /programs/swlib and /software/swlib, then create two separate archives, one for each configured directory. In this case, create programs_swlib.zip and software_swlib.zip, respectively.</p>	

Table 5–1 (Cont.) Upgrading Enterprise Manager with 2-System Upgrade Approach

Step No.	Step	Procedure
(f)	<p>Back up your existing database, which houses the Management Repository, to a host that can be either a completely new host or the host where your existing OMS is running.</p> <p>Choose to back up the repository on the host where your existing OMS is running only if you have sufficient space to accommodate it.</p> <p>Then, create a new database instance out of it so that the repository configured in it can be upgraded.</p> <p><i>Note:</i></p> <ul style="list-style-type: none"> - Before backing up the database, ensure that you stop all the running and scheduled deployment procedures in your existing Enterprise Manager system. - If you back up the database using DBCA, then ensure that you unlock all the user accounts, except for MGMT_VIEW user, before installing Enterprise Manager Cloud Control. - <i>Do not back up the repository using the DB cloning feature in the Enterprise Manager console. If you do, then you will not see the cloned database discovered in the Enterprise Manager console.</i> - Any Management Agent or target added to the existing Enterprise Manager system after backing up the Management Repository will not be upgraded and will need to be manually added to the upgraded Enterprise Manager system. To identify the targets that need to be manually added to the upgraded system, see the diff report as described in Chapter 28. 	

Table 5–1 (Cont.) Upgrading Enterprise Manager with 2-System Upgrade Approach

Step No.	Step	Procedure
(g)	<p>On the backed up Management Repository, meet the following prerequisites:</p> <ul style="list-style-type: none"> ■ Ensure that the MGMT_CONNECTOR_CONFIG table does not have any NULL rows. To verify this, run the following SQL query. <pre>select * from mgmt_cntr_config where connector_type_guid IS NULL and connector_guid IS null;</pre> <p>Typically, the command must not return any rows. If it does return any rows, then run the following SQL query to clean the table:</p> <pre>delete from mgmt_cntr_config where connector_guid IS NULL or connector_type_guid IS NULL; commit;</pre> ■ Ensure that there are no custom-created materialized views in the Management Repository. To verify this, run the following SQL query. Typically, the command must not return any rows. If it does return any rows, then contact Oracle Support. <pre>select count(1) from ALL_MVIEW_LOGS where log_owner=<EM_REPOS_USER></pre> ■ Ensure that the tables do not have any snapshots created. To verify this, log in to the Management Repository and run the following SQL query as SYSMAN user: <pre>select master , log_table from all_mview_logs where log_owner='<EM_REPOS_USER></pre> <p>For example,</p> <pre>select master , log_table from all_mview_logs where log_owner='SYSMAN'</pre> <p>If there are snapshots created in a table, then the query displays the master table and the snapshot details. For example,</p> <pre>SQL> master log_table em-violations em\$violation_log</pre> <p>If there are snapshots, then drop them by running the following command as SYSMAN user:</p> <pre>SQL> Drop snapshot log on <master></pre> <p>For example,</p> <pre>SQL> Drop snapshot log on em-violations</pre> 	
(h)	<p>Remove the emkey from the Management Repository by running the following command from the old OMS home:</p> <pre>\$<OMS_HOME>/bin/emctl config emkey -remove_from_repos [-sysman_pwd <pwd>]</pre>	

Table 5–1 (Cont.) Upgrading Enterprise Manager with 2-System Upgrade Approach

Step No.	Step	Procedure
(i)	Provide the date and time when the Management Repository was backed up. <i>Note:</i> Any Management Agent or target added to the existing Enterprise Manager system after backing up the Management Repository will not be upgraded and will need to be manually added to the upgraded Enterprise Manager system. To identify the targets that need to be manually added to the upgraded system, see the diff report as described in Chapter 28 .	Chapter 15
(j)	Install Enterprise Manager Cloud Control on the remote host and upgrade the Management Repository in the database you backed up in Step 3 (f). You can choose to install in graphical or silent mode. You can also choose to install the software binaries at one point and upgrade them later in graphical or silent mode.	Chapter 16 , Chapter 17 , Chapter 18 , or Chapter 19
(k)	Link the earlier release of the Management Repository with the upgraded Management Repository.	Chapter 22
(l)	<i>(Only if your old Enterprise Manager had Software Library configured)</i> Reconfigure the Software Library in Enterprise Manager Cloud Control so that it is independent of the Software Library configured for the old Enterprise Manager system.	Chapter 23
Step 4	Upgrade Oracle Management Agent	
(a)	Deploy and configure the software binaries of Oracle Management Agent 12c.	Chapter 11
(b)	Generate a health report and check the readiness of the predeployed Management Agents.	Chapter 12
(c)	Verify and sign off the health check report.	Chapter 13
(d)	Switch over the old Management Agents to the newly deployed ones so that they can communicate with Enterprise Manager Cloud Control. <i>Note:</i> If you have a large number of agents, then you can choose to upgrade one set of Oracle Management Agents in one attempt, and the next set in the subsequent attempt. In this case, you can repeat Step 4 (a) to Step 4 (d) for each attempt.	Chapter 14
Step 5	Perform Postupgrade Task	
(a)	Check the agent upgrade status	Chapter 24
(b)	Perform the general post-upgrade tasks.	Chapter 25
(c)	Track the status of deferred data migration jobs.	Chapter 26
(d)	Track the status of accrued data migration jobs.	Chapter 27
(e)	Generate diff reports to identify all configuration or setup-related changes that were manually made to the earlier release of the Enterprise Manager system while it was being upgraded.	Chapter 28
(f)	View a list of targets that are currently inactive in the upgraded Enterprise Manager system.	Chapter 29
(g)	Sign off accrued data migration process.	Chapter 30
(h)	Update the incident rules for metrics associated with the OMS.	Chapter 31

Table 5–1 (Cont.) Upgrading Enterprise Manager with 2-System Upgrade Approach

Step No.	Step	Procedure
(i)	<p data-bbox="586 260 1170 317"><i>(Only if you have Application Dependency and Performance (ADP) or JVM Diagnostics (JVMD) installed)</i></p> <ol style="list-style-type: none"> <li data-bbox="586 327 1208 464">1. If you have not deinstalled the JVMD and ADP applications from your inventory by logging into the WebLogic Administration Console for each monitored domain and removing the <i>jamagent</i> and <i>Acsera</i> application deployments, then do so now. <li data-bbox="586 474 1224 716">2. Delete all <i>ad4jTarget</i> targets: <ol style="list-style-type: none"> <li data-bbox="634 516 1036 541">(a) Navigate to the following location: <middleware_home>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.1.0/archives/jvmd/ <li data-bbox="634 642 948 667">(b) Extract the file <i>jvmd.zip</i>. <li data-bbox="634 684 1224 709">(c) Run the script <i>jvmd_targetupgrade11_12.sql</i>. <li data-bbox="586 726 1224 968">3. Delete all <i>OCAMM Manager</i> targets: <ol style="list-style-type: none"> <li data-bbox="634 768 1036 793">(a) Navigate to the following location: <middleware_home>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.1.0/archives/ocamm/ <li data-bbox="634 894 1036 919">(b) Extract the file <i>ADPManager.zip</i>. <li data-bbox="634 936 1203 961">(c) Run the script <i>adp_targetupgrade11_12.sql</i>. <li data-bbox="586 978 1057 1003">4. Deploy new JVMD and ADP managers. <li data-bbox="586 1020 1170 1073">5. Deploy new JVMD and ADP agents based on your inventory. 	

Upgrading with 1-System Approach on a Different Host

To upgrade your existing Enterprise Manager system to Enterprise Manager Cloud Control with 1-System upgrade approach on a different host, follow these steps:

Table 6–1 *Upgrading Enterprise Manager with 1-System Upgrade Approach on a Different Host*

Step No.	Step	Procedure
Step 1	Prepare Yourself	
(a)	Learn about the 1-System upgrade approach on a different host.	Chapter 2
(b)	Review the important facts you need to know before you begin.	Chapter 3
Step 2	Perform Preupgrade Tasks	
(a)	Apply the preupgrade console patch on your existing Enterprise Manager system to get access to the Enterprise Manager 12c Upgrade Console.	Section 2.2.1
(b)	Provide information about the host where you plan to upgrade your existing OMS.	Chapter 8
(c)	Manually download the following software, and stage them to an accessible location: <ul style="list-style-type: none"> ▪ Oracle Management Agent 12c ▪ All the required plug-ins 	Section 3.5.1
(d)	Provide information about the location of the software you manually downloaded and staged in Step 2 (c).	Chapter 9
(e)	Analyze your environment to identify Oracle Management Agents (Management Agent) with valid and invalid inventory, check their upgradability status, and identify the problematic Management Agents. If a required software is missing, then repeat Step (c) and Step (d).	Chapter 10
(f)	Meet the prerequisites for upgrading the Management Agents.	Appendix D
Step 3	Upgrade Oracle Management Agent	
(a)	Deploy and configure the software binaries of Oracle Management Agent 12c.	Chapter 11
(b)	Generate a health report and check the readiness of the predeployed Management Agents.	Chapter 12

Table 6–1 (Cont.) Upgrading Enterprise Manager with 1-System Upgrade Approach on a Different Host

Step No.	Step	Procedure
(c)	Verify and sign off the health check report.	Chapter 13
(d)	<p>Switch over the old Management Agents to the newly deployed ones so that they can communicate with Enterprise Manager Cloud Control.</p> <p><i>Note: If you have a large number of agents, then you can choose to upgrade one set of Oracle Management Agents in one attempt, and the next set in the subsequent attempt. In this case, you can repeat Step 3 (a) to Step 3 (d) for each attempt.</i></p>	Chapter 14
Step 4	Upgrade Oracle Management Service and Oracle Management Repository	
(a)	<p>On the remote host where you plan to install Enterprise Manager Cloud Control, meet the following prerequisites:</p> <ul style="list-style-type: none"> ■ Meet the Oracle Management Service-related prerequisites described in the chapter on installing Enterprise Manager Cloud Control, in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i>. ■ Meet the Management Agent-related prerequisites described in Appendix D. ■ Meet these additional requirements: <ul style="list-style-type: none"> If you have Power Broker set up, then disable the welcome message. If you have SUDO set up, then ensure that you have SUDO privileges to invoke <code>/bin/sh</code> as <code>root</code>. Ensure that you have the line <code>Defaults visiblepw</code> in the <code>/etc/sudoers</code> file. Also ensure that you comment out the line <code>Defaults requiretty</code> in the file. 	

Table 6–1 (Cont.) Upgrading Enterprise Manager with 1-System Upgrade Approach on a Different Host

Step No.	Step	Procedure
(b)	<p>On the Management Repository, meet the following prerequisites:</p> <ul style="list-style-type: none"> ■ Ensure that the MGMT_CONNECTOR_CONFIG table does not have any NULL rows. To verify this, run the following SQL query. <pre>select * from mgmt_cntr_config where connector_type_guid IS NULL and connector_ guid IS null;</pre> <p>Typically, the command must not return any rows. If it does return any rows, then run the following SQL query to clean the table:</p> <pre>delete from mgmt_cntr_config where connector_guid IS NULL or connector_type_ guid IS NULL;</pre> <pre>commit;</pre> ■ Ensure that there are no custom-created materialized views in the Management Repository. To verify this, run the following SQL query. Typically, the command must not return any rows. If it does return any rows, then contact Oracle Support. <pre>select count(1) from ALL_MVIEW_LOGS where log_owner=<EM_REPOS_USER></pre> ■ Ensure that the tables do not have any snapshots created. To verify this, log in to the Management Repository and run the following SQL query as SYSMAN user: <pre>select master , log_table from all_mview_ logs where log_owner='<EM_REPOS_USER></pre> <p>For example,</p> <pre>select master , log_table from all_mview_ logs where log_owner='SYSMAN'</pre> <p>If there are snapshots created in a table, then the query displays the master table and the snapshot details. For example,</p> <pre>SQL> master log_table em-violations em\$violation_log</pre> <p>If there are snapshots, then drop them by running the following command as SYSMAN user:</p> <pre>SQL> Drop snapshot log on <master></pre> <p>For example,</p> <pre>SQL> Drop snapshot log on em-violations</pre> 	
(c)	<p>Stop all running and scheduled deployment procedures in your existing Enterprise Manager system before upgrading the system.</p>	

Table 6–1 (Cont.) Upgrading Enterprise Manager with 1-System Upgrade Approach on a Different Host

Step No.	Step	Procedure
(d)	<p><i>(Only if you have Application Dependency and Performance (ADP) or JVM Diagnostics (JVMD) installed)</i></p> <ol style="list-style-type: none"> 1. Take an inventory of the JVMs and WebLogic Domains being monitored by JVMD and/or ADP. 2. Deinstall the JVMD and ADP applications from your inventory by logging into the WebLogic Administration Console for each monitored domain and removing the <i>jamagent</i> and <i>Acsera</i> application deployments. 3. Shut down all of your ADP and JVMD managers. 4. Remove all ADP and JVMD managed servers from the GCDomain using the WebLogic Administration Console. 5. Run purge scripts for JVMD: <ol style="list-style-type: none"> (a) Navigate to the following location: <code><middleware_home>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.1.0/archives/jvmd/</code> (b) Extract the file <code>jvmd.zip</code>. (c) Run the script <code>jvmd_monitoringupgrade11_12.sql</code>. (d) Run the script <code>jvmd_traceupgrade11_12.sql</code> if there are existing Thread Snapshots from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1). 	
(e)	<p>Copy the emkey from the OMS to the Management Repository:</p> <ul style="list-style-type: none"> ■ If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5), then run the following command from the OMS home: <code>\$<OMS_HOME>/bin/emctl config emkey -copy_to_repos -sysman_pwd <sysman_pwd></code> ■ If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), then run the following command from the OMS home: <code>\$<OMS_HOME>/bin/emctl config emkey -copy_to_repos_from_file -repos_host <repository_host> -repos_port <port> -repos_sid <sid> -repos_user <username> [-repos_pwd <pwd>] [-admin_pwd <pwd>] -emkey_file <OMS_HOME>/sysman/config/emkey.ora</code> 	
(f)	<p>If you have a Server Load Balancer (SLB) configured, then make changes to your monitors.</p>	<p>Appendix E</p>

Table 6–1 (Cont.) Upgrading Enterprise Manager with 1-System Upgrade Approach on a Different Host

Step No.	Step	Procedure
(g)	<p>If your old Enterprise Manager has Oracle Software Library (Software Library) configured on a shared, NFS-mounted drive, then ensure that the shared drive is accessible from the remote host where you plan to install Enterprise Manager Cloud Control.</p> <p>However, if the Software Library is configured on the local system where the existing, earlier release of Enterprise Manager is running, then copy the Software Library to the remote host where you plan to install Enterprise Manager Cloud Control, in the same directory path as the one maintained in the old Enterprise Manager system.</p>	
(h)	Install Enterprise Manager Cloud Control on the remote host and upgrade the Management Repository in the existing database.	Chapter 20
Step 5	Perform Postupgrade Task	
(a)	Check the agent upgrade status.	Chapter 24
(b)	Perform the general post-upgrade tasks.	Chapter 25
(c)	Track the status of deferred data migration jobs.	Chapter 26
(d)	Update the incident rules for metrics associated with the OMS.	Chapter 31
(e)	<p><i>(Only if you have Application Dependency and Performance (ADP) or JVM Diagnostics (JVMD) installed)</i></p> <ol style="list-style-type: none"> If you have not deinstalled the JVMD and ADP applications from your inventory by logging into the WebLogic Administration Console for each monitored domain and removing the <i>jamagent</i> and <i>Acsera</i> application deployments, then do so now. Delete all <i>ad4jTarget</i> targets: <ol style="list-style-type: none"> Navigate to the following location: <pre><middleware_home>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.1.0/archives/jvmd/</pre> Extract the file <i>jvmd.zip</i>. Run the script <i>jvmd_targetupgrade11_12.sql</i>. Delete all <i>OCAMM Manager</i> targets: <ol style="list-style-type: none"> Navigate to the following location: <pre><middleware_home>/plugins/oracle.sysman.emas.oms.plugin_12.1.0.1.0/archives/ocamm/</pre> Extract the file <i>ADPManager.zip</i>. Run the script <i>adp_targetupgrade11_12.sql</i>. Deploy new JVMD and ADP managers. Deploy new JVMD and ADP agents based on your inventory. 	

Part III

Preupgrade Requirements

This part describes the preupgrade requirements you must meet. In particular, this part covers the following:

- [Chapter 8, "Identifying Host for Enterprise Manager Cloud Control"](#)
- [Chapter 9, "Managing Software"](#)
- [Chapter 10, "Analyzing Your Environment"](#)

Configuring Postupgrade Tasks

Note: Follow these instructions only if you are upgrading using the 1-System upgrade approach. Perform these steps in the Enterprise Manager Grid Control console of the earlier release.

By default, soon after the upgrade, Enterprise Manager Cloud Control automatically runs the deferred data migration process (DDMP) jobs. These jobs migrate historical data such as metrics, configuration, and so on from the format stored in the earlier release of Enterprise Manager to the format compatible with Enterprise Manager Cloud Control. For more information DDMP jobs, see [Chapter 26](#).

Depending on the size of your Enterprise Manager system, these jobs consume a high amount of Management Repository resources and take longer time to complete. In particular, when you upgrade using the 1-System upgrade approach, you might face resource contention as all the Management Agents will be up and running soon after the upgrade.

For better control on these jobs, you may choose to disable the auto-run of these DDMP jobs. If you do so, you must run these jobs later explicitly from the Post Upgrade Tasks page within the Enterprise Manager Cloud Control console.

To disable the auto-run of DDMP jobs, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Select Upgrade Type section, select **1-System**.

Enterprise Manager Grid Control refreshes the page and displays a table with a list of tasks you need to perform for the upgrade approach you selected.

4. In the Preupgrade Steps section, from the table, click **Configure Postupgrade Tasks**.
5. On the Configure Postupgrade Tasks page, select **Disable automatic DDMP jobs**.
6. Click **Save**.

Enterprise Manager Grid Control saves the information you provided and returns to the Upgrade Console page that shows a list of tasks to perform for the upgrade approach you selected.

Note: If you want to run the DDMP jobs explicitly after upgrading to Enterprise Manager Cloud Control, perform Step (3) as described in [Section 26.2](#)—select each component and click **Start**.

Identifying Host for Enterprise Manager Cloud Control

Note: Follow these instructions only if you are upgrading using the 2-System upgrade approach or the 1-System upgrade approach on a different host. Perform these steps in the Enterprise Manager Grid Control console of the earlier release.

To identify and provide information about the host where you plan to install Enterprise Manager Cloud Control, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Select Upgrade Type section, select one of the following.
 - To upgrade your Enterprise Manager system with "near zero" downtime (even if you manually install Management Agents), select **2-System**.
 - To upgrade your Enterprise Manager system with downtime on a different host, select **1-System on a Different Host**.

Enterprise Manager Grid Control refreshes the page and displays a table with a list of tasks you need to perform for the upgrade approach you selected.

4. In the Preupgrade Steps section, from the table, click **Identify Host and Port for New Enterprise Manager System**.
5. On the Identify Host and Port for New Enterprise Manager System page, enter the following:
 - The fully qualified name of the host where you plan to install Enterprise Manager Cloud Control. For example, `example.com`.
 - The secure port and the unsecure upload port you plan to assign for that Enterprise Manager Cloud Control console. For example, `1768`.

In case of a multi-OMS environment, if the host on which you plan to install Oracle Management Service 12c is managed by a Server Load Balancer (SLB), then select **Click if you wish to have Server Load Balancer (SLB) configured for your Oracle Management Service 12c Release 1 (12.1.0.1.0)**. Then, enter the fully qualified name, and the secure and unsecure upload ports of the host where the SLB is running.

Note:

- For 2-System upgrade approach and 1-System upgrade approach on a different host, understandably, the host referred to here is any host other than the one where your existing OMS is running. In a Multi-OMS environment this means that a new virtual host name must be used and a new SLB configuration created for this virtual host name.
- Ensure that you install Oracle Management Service 12c on the host entered here, and ensure that you use the same HTTPS and HTTP upload ports entered here. In the installation wizard, on the Port Configuration Details screen, enter the HTTPS upload port for the component **Enterprise Manager Upload Http SSL Port**, and the HTTP upload port for the component **Enterprise Manager Upload Http Port**.

If you have already installed Oracle Management Service 12c, then retrieve the values from the `emgc.properties` file, which is available in the OMS home. For HTTPS upload port, look for the value assigned to the parameter `EM_UPLOAD_HTTPS_PORT`, and for HTTP upload port, look for the value assigned to the parameter `EM_UPLOAD_HTTP_PORT`.

- Once you enter the secure and unsecure upload ports here, avoid changing them once the deployment starts.
-
-

6. In the Configure Postupgrade Tasks section, select one of the following options:

- **Disable automatic DDMP jobs**, if you want to prevent the DDMP jobs from running automatically. This option is applicable for 1-System upgrade approach as well as 1-System upgrade approach on a different host.

If you want to run the DDMP jobs explicitly after upgrading to Enterprise Manager Cloud Control, perform Step (3) as described in [Section 26.2](#)—select each component and click **Start**.

Note: If you disable the DDMP jobs, the ADMP jobs are also disabled by default.

- **Disable automatic ADMP jobs**, if you want to prevent the ADMP jobs from running automatically. This option is applicable only for 1-System upgrade approach.

If you want to run the DDMP jobs explicitly after upgrading to Enterprise Manager Cloud Control, perform Step (3) as described in [Section 27.2](#).

7. Click **Save**.

Enterprise Manager Grid Control saves the information you provided and returns to the Upgrade Console page that shows a list of tasks to perform for the upgrade approach you selected.

Managing Software

Note: Perform these steps in the Enterprise Manager Grid Control console of the earlier release.

To manage information about the location of the core Management Agent software and its associated plug-ins, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Select Upgrade Type section, select one of the following. For information about these upgrade approaches, see "Understanding Upgrade Approaches".
 - To upgrade your Enterprise Manager system with downtime (even if you manually install Management Agents), select **1-System**.
 - To upgrade your Enterprise Manager system with "near zero" downtime (even if you manually install Management Agents), select **2-System**.
 - To upgrade your Enterprise Manager system with downtime on a different host, select **1-System on a Different Host**.

Enterprise Manager Grid Control refreshes the page and displays a table with a list of tasks you need to perform for the upgrade approach you selected.

4. In the Preupgrade Steps section, from the table, click **Manage Software**.
5. On the Manage Software page, in the Agent Upgradability and Target Upgradability pie charts, click the hyperlinks in the respective legends and identify the Management Agents and targets that can be upgraded, and that cannot be upgraded due to unavailability of the Management Agent software or the plug-in software.
6. In the Provide Software Location section, enter the absolute path to the directory where the core Management Agent software and the plug-in software are present for the required platforms.

For example, `/john/software/oracle/em/`.

And then, click **Validate** to register that location with the Enterprise Manager system.

Note:

- The absolute path you enter must be to a staging location that contains both the Management Agent software and the plug-in software.

To download the Management Agent software and the plug-ins, follow these steps

(a) Access the following URL:

<http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html>

(b) Download the Management Agent software to an accessible location. Do NOT extract the contents of the software ZIP file. The Management Agent software is platform-specific, so ensure that you copy the software for the platform on which you want to install.

(c) Download all the required plug-ins to the same location. Plug-ins are generic, so they are common for all platforms.

Ensure that you download all the plug-ins listed as required plug-ins on the Manage page, whether or not you want to monitor a target with them. You may feel that a few plug-ins are not required because you do not have targets to be monitored by them, but those plug-ins may be required for upgrading your system. Therefore, download all the plug-ins listed on the Manage Software page. Ensure that you download these plug-ins before backing up the database that contains the Management Repository.

- After registering the locations of the Management Agent software and the plug-in software, if you download some more plug-ins at a later stage in the same or a different location, then register the location of those recently downloaded plug-ins as well.
 - The validation and registration process might take some time to complete, so after you click **Validate**, wait for some time for the process to end. Once the process ends, you should see a message confirming that the location has been successfully registered.
 - If you plan to install multiple Oracle Management Services (OMSes), then ensure that the location you enter is writable and accessible to all the OMSes.
-
-

Analyzing Your Environment

This chapter describes how you can analyze your existing Oracle Management Agents (Management Agent) and prepare yourself to upgrade them. In particular, this chapter covers the following:

- [Identifying Management Agents with Valid Inventory](#)
- [Identifying Management Agents with Invalid Inventory](#)
- [Checking the Upgradability Status of Oracle Management Agents](#)
- [Checking the Upgradability Status of Targets](#)
- [Identifying Problematic Oracle Management Agents](#)
- [Identifying Management Agents That Need to Be Reconfigured](#)

Note: Perform these steps in the Enterprise Manager Grid Control console of the earlier release.

10.1 Identifying Management Agents with Valid Inventory

Every Oracle software product, including Oracle Management Agent (Management Agent) installed on a host is registered with the central inventory (*oraInventory*). Every Oracle software product has an entry in the `inventory.xml` file, which is present in the *oraInventory* directory. If a Management Agent is registered with the central inventory, then it is a Management Agent with valid inventory.

To identify Management Agents with valid inventory, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Agent Upgrade Status section, view the count displayed against **Agents with Valid Inventory**.

To drill down and view more information about each of the Management Agents, click the count value.

Enterprise Manager Grid Control displays the Upgrade Status page that provides information such as the platform on which the Management Agents are running; their versions; their old and new Oracle home locations; and their deployment, configuration, health check, and switch over status.

Note:

- The count displayed here does not include the Management Agents with invalid inventory and the Management Agents that were installed after the count was determined.
 - To consider the Management Agents that have an invalid inventory, first resolve the issue with such Management Agents. Ensure that there are no such faulty Management Agents. For information on how to identify such Management Agents and resolve them, see [Section 10.2](#). Once you have resolved the issue, click **Refresh Agents and Targets List**.
 - To consider the Management Agents that were installed after the count was determined, refresh the list by clicking Refresh Agents and Targets List.
-

10.2 Identifying Management Agents with Invalid Inventory

Every Oracle software product, including Management Agent installed on a host is registered with the central inventory (*oraInventory*). Every Oracle software product has an entry in the `inventory.xml` file, which is present in the *oraInventory* directory.

However, there may be circumstances when an entry for a Management Agent might be missing, incomplete, or corrupt, or the entry might be existing with an incorrect syntax. In addition, there is also a possibility that the host configuration was not refreshed and the latest configuration was not collected. If a Management Agent is not registered with the central inventory for such reasons, then it is a Management Agent with invalid inventory.

Management Agents with invalid inventory do not appear in the *Enterprise Manager 12c Upgrade Console*, and as a result, you will not be able to upgrade them until the issues are fixed.

To identify Management Agents with invalid inventory, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Agent Upgrade Status section, view the count displayed against **Agents with Invalid Inventory**.

To drill down and view more information about each of the Management Agents, click the count value.

Note: To resolve this issue, follow these steps:

1. Check the entry for these Management Agents in the `inventory.xml` file.

The `inventory.xml` file is present in the `oraInventory` directory (central inventory). The location the `oraInventory` directory is mentioned in the `oraInst.loc` file that you pass while invoking the installer in silent mode. Ensure that the entry is present with the correct syntax.

2. Refresh the host configuration in one of the following ways:
 - (a) Go to the home page of the host. Click the **Configuration** tab. On the Configuration page, click **Refresh**.
 - (b) Go to the Deployments page. In the Configuration section, click **Refresh Host Configuration**.

If Step 2 (a) or Step 2 (b) fail, then run the following command from the Management Agent home:

```
$<AGENT_HOME>/bin/emctl control agent
runCollection
```

3. Refresh the agent list in the *Enterprise Manager 12c Upgrade Console*. Go to the upgrade console. In the Agent Upgrade Status section, click **Refresh Agents and Targets List**.
-
-

10.3 Checking the Upgradability Status of Oracle Management Agents

To check the upgradability status of the Management Agents, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Preupgrade Steps section, from the table, click **Manage Software**.
4. On the Manage Software page, view the Agent Upgradability pie chart. The pie chart graphically shows the following information:
 - **Completely Upgradable** - Number of Management Agents that can be fully upgraded because the Management Agent software and all the associated, target-specific management plug-in software are available.
 - **Missing Plug-Ins Software** - Number of Management Agents that can be partially upgraded because the Management Agent software and only a few of the associated, target-specific management plug-in software are available. Some management plug-in software are either missing or unsupported in the upgraded Enterprise Manager system.
 - **Missing Agent Software** - Number of Management Agents that cannot be upgraded because the Management Agent software is not available. The associated, target-specific management plug-in software might be available, but the core Management Agent software is not available.
 - **Not Supported** - Number of Management Agents that are not supported in the upgraded Enterprise Manager system because Oracle Management Agent 12c has not been released for a particular platform. The targets monitored by

those Management Agents can no longer be monitored in the upgraded Enterprise Manager system.

10.4 Checking the Upgradability Status of Targets

To check the upgradability status of the targets, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, do one of the following:
 - In the Other Links section, click **Targets Upgradability Status**.

On the Targets Upgradability Status page, use the search functionality to search and identify the targets that can either be monitored or not monitored in the upgraded Enterprise Manager system.

For example, to list the targets that cannot be monitored in the upgraded Enterprise Manager system, from the **Upgrade Status** list, select **Not Upgradable**. Similarly, to list the target that can be monitored, select **Upgradable**.

- In the Preupgrade Steps section, from the table, click **Manage Software**.

On the Manage Software page, view the Target Upgradability pie chart. The pie chart graphically shows the following information:

- **Upgradable** - Number of targets that can be monitored in the upgraded Enterprise Manager system because the Management Agent software and the associated, target-specific management plug-in software are available.
- **Missing Agent/Plug-In Software** - Number of targets that cannot be monitored in the upgraded Enterprise Manager system because either the Management Agent software is missing or the associated management plug-in software is missing.
- **Not Supported** - Number of targets that cannot be monitored in the upgraded Enterprise Manager system because either Oracle Management Agent 12c has not been released for the platforms on which the targets are running, or the management plug-ins for those targets are not supported in the upgraded Enterprise Manager system.
- **Plug-In Software Not Certified** - Number of targets that cannot be monitored in the upgraded Enterprise Manager system because the management plug-ins for those targets are not certified.

10.5 Identifying Problematic Oracle Management Agents

There may be Management Agents that cannot be upgraded due to technical issues such as missing host target, association with multiple host targets, unreachable state, invalid inventory, and so on.

To identify such problematic Management Agents, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.

3. On the Upgrade Console page, in the Other Links section, click **Problematic Agents**.
4. On the Problematic Agents page, view the Management Agents that cannot be upgraded.
 - To search for a particular Management Agent, enter the Management Agent name in the **Agent Name** field, and click **Search**.
 - To filter the Management Agents based on a particular technical reason, select one of the following reasons from the **Reason** list, and click **Search**:
 - **Missing Repository Inventory** - Lists the Management Agents that are not registered with the central inventory (*oraInventory*).
 - **Multiple Host Target** - Lists the Management Agents that are either associated with or monitoring more than one host.
 - **Agent Unreachable** - Lists the Management Agents that are down.
 - **Host Target Missing** - Lists the Management Agents whose hosts are not discovered and monitored in the Enterprise Manager Grid Control console. The Management Agents themselves may be monitored but their hosts may not be monitored for some reason.
 - **All** - Lists all the Management Agents that have one or more issues listed in the **Reason** list.

10.6 Identifying Management Agents That Need to Be Reconfigured

You might have to reconfigure the Management Agents for one of the following reasons:

- If the OMS host and port with which you deployed a Management Agent do not match with the OMS host and port with which you deployed the other Management Agents.
- You have either deleted one or more targets monitored by this Management Agent, or added new targets to be monitored by this Management Agent. To resolve this issue, reconfigure this Management Agent so that the new configuration can take effect.
- The versions of the plug-ins you deployed with this Management Agent are different from the versions of the plug-ins you deployed with the other Management Agents. To resolve this issue, deploy this Management Agent again with the correct plug-in versions.

To identify the Management Agents that need to be reconfigured, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Other Links section, click **Agents Needing Reconfiguration**.
4. On the Agents Needing Reconfiguration page, view the Management Agents that need to be reconfigured. The table not only lists the Management Agents but also provides the following reasons for you to reconfigure them.
 - OMS Host and Port Mismatch

Indicates that the OMS host and port with which you deployed the Management Agent do not match with the OMS host and port with which you deployed the other Management Agents. To resolve this issue, access the Identify Host and Port for New Enterprise Manager System page, correct the OMS host and port, and deploy this Management Agent again.

- **Targets Deleted or Added**

Indicates that you have either deleted one or more targets monitored by this Management Agent, or added new targets to be monitored by this Management Agent. To resolve this issue, reconfigure this Management Agent so that the new configuration can take effect.

- **Plug-In Version Mismatch**

Indicates that the versions of the plug-ins you deployed with this Management Agent are different from the versions of the plug-ins you deployed with the other Management Agents. To resolve this issue, deploy this Management Agent again with the correct plug-in versions.

Part IV

Upgrading Oracle Management Agent

This part describes how you can upgrade your Oracle Management Agents. In particular, this part covers the following:

- [Chapter 11, "Deploying and Configuring Oracle Management Agent"](#)
- [Chapter 12, "Generating Health Report of Deployed Oracle Management Agents"](#)
- [Chapter 13, "Verifying and Signing Off the Health Report of Deployed Oracle Management Agents"](#)
- [Chapter 14, "Switching Over to Oracle Management Agent 12c"](#)

Deploying and Configuring Oracle Management Agent

To deploy Oracle Management Agent 12c, follow these steps:

Note:

- Perform these steps in the Enterprise Manager Grid Control console of the earlier release.
- You cannot deploy and configure Oracle Management Agent 12c for problematic Management Agents. To identify the problematic Management Agents, see [Section 10.5](#).
- Also, you must deploy and configure Oracle Management Agent 12c only on existing Management Agents that are completely upgradable. To identify whether the Management Agents are completely upgradable, see [Section 10.3](#).
- For the 2-System upgrade, do NOT deploy Oracle Management Agent 12c on the remote host because the Enterprise Manager installer will take care of installing it while installing Oracle Management Service 12c.
- For 2-System upgrade, if your old Management Agent was running in secure (or unsecure) mode before backing up the Management Repository, then ensure that it continues to run in the same mode while you deploy and configure the new Management Agent for it. Do not resecure the Management Agents after backing up the Management Repository. If you do so, the ping test might fail while performing the healthcheck because of a mismatch between the configuration stored in the repository and the actual configuration of the Management Agent. You will see a KEY_MISMATCH error in `gcagent.log`. For information on this error and to know how to secure the Management Agents without facing this issue, see [Appendix H](#).

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Select Upgrade Type section, select one of the following. For information about these upgrade approaches, see "Understanding Upgrade Approaches".

-
- To upgrade your Enterprise Manager system with downtime (even if you manually install Management Agents), select **1-System**.
 - To upgrade your Enterprise Manager system with "near zero" downtime (even if you manually install Management Agents), select **2-System**.
 - To upgrade your Enterprise Manager system with downtime on a different host, select **1-System on a Different Host**.

Enterprise Manager Grid Control refreshes the page and displays a table with a list of tasks you need to perform for the upgrade approach you selected.

4. In the Preupgrade Steps section, from the table, click **Deploy and Configure Agents**.
5. On the Deploy and Configure Agents page, for **Operation Name**, enter a unique name for the deployment operation you are about to perform. The custom name you enter can be any intuitive name, and need not necessarily be in the same format as the default name.

For example, `Deploy_Agents_Phase1_2010_12_23`.

Note: The operation name you enter here is only a logical name and will be used for saving the details of the operation you are about to perform. After deploying the software binaries of Oracle Management Agent 12c, at a later point in time, if you want to check the health of the deployed Management Agents or switch over from old to newly deployed and configured Management Agents, then you can use the operation name to identify and track the Management Agents selected as part of this operation.

6. In the Select Operation Type section, select **Deploy Agent and Plug-In Software and Configure Agent and Plug-In Software**.

Note: If you had already deployed the software binaries of the Management Agent, then you can choose to only configure them now. In this case, select only **Configure Agent and Plug-In Software**.

7. In the Search Agents section, search and add the existing, old Management Agents for which you want to deploy the software. To understand how to search and add Management Agents, see [Appendix G](#).

Note:

- If you had already deployed the software binaries of the Management Agent, and if you are only configuring them at this point, then search (or add) and select the Management Agents for which you had already manually deployed the software.
 - If you are adding a *Shared Agent*, then ensure that you add the *Master Agent* to which it communicates, and all the *Shared Agents* that communicate with this *Master Agent*.
 - When you return to this screen to retry the deploy operation, you will see the Management Agents selected as part of the previous deploy operation. This is an expected behavior. You can choose to redeploy the software binaries for them, or remove them from the list and add a fresh set of Management Agents.
-
-

8. In the table that lists the Management Agents, enter an installation base directory and an instance home directory for each of the Management Agents.

Note:

- Ensure that the installation base directory you enter here is NOT inside the middleware home.
 - Ensure that the installation base directory has at least 110 MB of free disk space.
 - If you had already deployed the software binaries of the Management Agent, and if you are only configuring them at this point, then enter the same installation base directory and the instance home directory where you had deployed the software binaries.
-
-

If you want the paths to the installation base directory and the instance home directory to be the same across Management Agents, then select **Use Same Paths for All Agents**, and enter the absolute path for installation base directory and instance home directory, just once, for the first Management Agent listed in the table. Enterprise Manager Grid Control will consider the same paths for other Management Agents listed in the table.

Note: You cannot select **Use Same Paths for All Agents** with the installation base directory mentioned for one Management Agent and the instance home directory mentioned for another Management Agent in the table. Only the paths specified for the first Management Agent will be considered as the same paths for other Management Agents in the table.

If the agent base directory or the agent instance home directory specified by you already exists, and if you want to overwrite them, then select **Overwrite Any Existing Directories**. Typically, you will select this option when you choose to redeploy the software binaries in the same base directory.

9. After you add the Management Agents, select each of them from the **Select** column.

-
10. In the Agent Credentials section, retain the default selection, that is, **Use Oracle Home Preferred Credentials**, so that the preferred credentials stored in the Management Repository can be used for this job.

Note: Ensure that the preferred credentials were registered with the Enterprise Manager system using the Enterprise Manager Command Line Interface (EM CLI). For more information, see [Section F](#).

You can optionally override these preferred credentials. To do so, select **Override Oracle Home Preferred Credentials** and enter one set of credentials that can be used for all Oracle homes.

Note: Ensure that you use the same credentials that you used for the existing, earlier release of the Management Agent

11. In the Run Privilege section, by default, **None** is selected assuming that the credentials you have provided in the previous step have the privileges to run this job.

However, if those credentials do not have the privileges to run this job, and if you want to switch over as another user for this purpose, then select either **SUDO** or **Power Broker**, depending on the authentication utility you want to use, and provide the user account name and profile.

12. In the OMS Host and Port section, validate the name and the secure port of the host where you plan to install Oracle Management Service 12c. To change the values, click **Edit**.

Note: If you had already upgraded your existing OMS to Oracle Management Service 12c, then ensure that the port you enter here matches with the *Enterprise Manager Upload HTTP SSL Port* you selected or specified in the installer while upgrading the OMS.

13. Click **Next**.

14. On the Optional Details page, in the Pre-Deploy Options section, select **Run Pre-Command/Script** if you want to run any script before deploying the software binaries of the Management Agents.

Enter the absolute path to a location on the destination host where the script is available. The script can also be in a shared location, but you must have execute privileges on it to run the script.

Note: By default, the credentials provided in Step (10) are used for running the script. And by default, **None** is selected assuming that the credentials have the privileges to run the script.

However, if those credentials do not have the privileges to run the script, and if you want to switch over as another user for this purpose, then select either **SUDO** or **Power Broker**, depending on the authentication utility you want to use, and provide the user account name and profile.

-
15. In the Post-Config Options section, select **Run Post-Command/Script** if you want to run any script after configuring the deployed Management Agents.

Enter the absolute path to a location on the destination host where the script is available. The script can also be in a shared location, but you must have execute privileges on it to run the script.

Note: By default, the credentials provided in Step (10) are used for running the script. And by default, **None** is selected assuming that the credentials have the privileges to run the script.

However, if those credentials do not have the privileges to run the script, and if you want to switch over as another user for this purpose, then select either **SUDO** or **Power Broker**, depending on the authentication utility you want to use, and provide the user account name and profile.

16. (*Only for UNIX*) In the Root Credentials section, enter the credentials of a user account to run the `root.sh` script.

Note: By default, **None** is selected assuming that the credentials have the privileges to run the script.

However, if those credentials do not have the privileges to run the script, and if you want to switch over as another user for this purpose, then select either **SUDO** or **Power Broker**, depending on the authentication utility you want to use, and provide the user account name and profile.

17. Click **Submit**.

Note:

- After you submit the operation, if you see the following error, then first run `root . sh` from the old Management Agent home, and then, resubmit this operation.

```
ERROR: NMO not setuid-root (Unix-only)
```

- If you see the following error, then verify the credentials entered in Step (10).

```
Local Authentication Failed...Attempt PAM authentication...PAM failed . . .
```

- If the deployment operation fails at some point, you can choose to only reconfigure the Management Agents, and not copy the software binaries all over again. To only reconfigure the Management Agents, repeat the instructions outlined in this procedure, but for Step (6) ensure that you select only **Configure Agent and Plug-In Software**.
 - When the operation is in progress, if a Management Agent being deployed and configured becomes unavailable for some reason, you may see the status *Suspended on Event*. Once the Management Agent becomes available, the status automatically changes to show the current state. This is an expected behavior.
 - If the credentials entered in Step (10) are incorrect, then the step for running the `root . sh` script fails in the predeployment job, but the job as such shows that it is successful. In this case, manually run the `root . sh` script using the correct root credentials. Otherwise, the Management Agent will result in NMO errors.
-
-

Generating Health Report of Deployed Oracle Management Agents

Before you switch over from your old, existing Management Agent to the newly deployed and configured Oracle Management Agent 12c, generate a report to check the health and the readiness of the deployed Management Agents so that any issues with the deployment can be identified beforehand.

For all the Management Agents to switch over successfully and function properly in the upgraded Enterprise Manager system, you must ensure that the Management Agents are in a position to contact the upgraded Oracle Management Service, monitor all the targets they monitored before, and collect all the metrics details they collected before. The health report helps in identifying any issues related to these requirements so that you can resolve them beforehand.

Note: Perform these steps in the Enterprise Manager Grid Control console of the earlier release.

Note: You can generate health reports only for Management Agents that have been successfully deployed and configured.

To generate a health report of the deployed Management Agents and check their readiness, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Agent Upgrade Steps section, from the table, click **Generate Health Report of Deployed Agents**.
4. On the Generate Health Report for Deployed Agents page, in the Provide Inputs section, do the following:
 - a. Enter a unique name for the deployment operation you are about to perform. The custom name you enter can be any intuitive name, and need not necessarily be in the same format as the default name.

For example, `CheckHealth_Agents_Phase1_2010_12_23`.

Note: The operation name you enter here is only a logical name and will be used for saving the details of the operation you are about to perform. After checking the health of the deployed Management Agents, at a later point in time, if you want to switch over from old to newly deployed and configured Management Agents, then you can use the operation name to identify and track the Management Agents selected as part of this operation.

- b.** If you want to perform the readiness check for the Management Agents you had previously deployed, then click the torch icon against **Load Agents from Previous Operations**, and select the operation you had submitted for deploying those Management Agents, click **Go**.

Enterprise Manager Grid Control populates the table in the Search Agents section with a list of Management Agents that are associated with the operation you selected.

- 5.** In the Search Agents section, search and add the Management Agents for which you want to perform the readiness check:
 - If you specified a readiness operation name as described in Step 4 (a), then search (or add) and select the existing, old Management Agents for which you have already deployed the software and for which you want to check the health now. To understand how to search and add Management Agents, see [Appendix G](#).
 - If you selected a deployment operation as described in Step 4 (b), then review the Management Agents that are displayed based on the operation you selected.
- 6.** After you add the Management Agents, select each of them from the **Select** column.
- 7.** In the Agent Credentials section, retain the default selection, that is, **Use Oracle Home Preferred Credentials**, so that the preferred credentials stored in the Management Repository can be used for this job.

Note: Ensure that the preferred credentials were registered with the Enterprise Manager system using the Enterprise Manager Command Line Interface (EM CLI). For more information, see [Appendix F](#).

You can optionally override these preferred credentials. To do so, select **Override Oracle Home Preferred Credentials** and enter one set of credentials that can be used for all Oracle homes.

Note: Ensure that you use the same credentials that you used for the existing, earlier release of the Management Agent

- 8.** Click **Submit**.

Note:

- After you submit the operation, if you see the following error, then first run `root.sh` from the old Management Agent home, and then, resubmit this operation.

```
ERROR: NMO not setuid-root (Unix-only)
```

- If you see the following error, then verify the credentials entered in Step (10).

```
Local Authentication Failed...Attempt PAM authentication...PAM failed . . .
```

- When the operation is in progress, if a Management Agent for which you are performing a readiness check becomes unavailable for some reason, you may see the status *Suspended on Event*. Once the Management Agent becomes available, the status automatically changes to show the current state. This is an expected behavior.
- If you were monitoring a SOA target in your earlier release of Enterprise Manager, then in the health report, you might see metric collection errors for the following metrics:
 - Top SOA SQL Queries
 - Dehydration Store Tables

As this stage, you can ignore these errors and proceed further. However, ensure that you provide the database credentials for this target as described in [Chapter 25](#).

Verifying and Signing Off the Health Report of Deployed Oracle Management Agents

Before you switch over from your old, existing Management Agent to the newly deployed and configured Oracle Management Agent 12c, verify and sign off the health report of deployed Management Agents.

For all the Management Agents to switch over successfully and function properly in Enterprise Manager Cloud Control, you must ensure that the Management Agents are in a position to contact the upgraded Oracle Management Service (OMS), monitor all the targets they monitored before, and collect all the metrics details they collected before. The health report helps in identifying any issues related to these requirements so that you can resolve them beforehand.

Note: Perform these steps in the Enterprise Manager Grid Control console of the earlier release.

To verify and sign off the health report, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Agent Upgrade Steps section, from the table, click **Sign Off Health Report for Deployed Agents**.
4. On the Sign Off Health Report for Deployed Agents page, view the health and the readiness details for each of the Management Agents.
 - Verify the **Ping Test** column, which indicates whether or not the deployed Oracle Management Agent 12c will be able to contact the upgraded OMS.

Note:

For 1-System upgrade, in the **Ping Test** column, you will see the value *N/A*.

For 2-System upgrade, you will see either *Passed* or *Failed*. The status *Passed* indicates that the ping test was successful, and the status *Failed* indicates that the test was unsuccessful. If you see the status *Failed* for any Management Agent, then do the following:

- Verify the OMS host name and OMS port entered in the Identify Host and Port for New Enterprise Manager System page.

Alternatively, verify the `REPOSITORY_URL` parameter in the following file. Here, `<Agent_Instance_Home>` refers to the 12c agent home.

```
<Agent_Instance_Home>/sysman/config/emd.properties
```

If the OMS host name and port are correct, then check for errors in the following log file:

```
<Agent_Instance_Home>/sysman/log/gcagent.log
```

- If any Management Agent is in unsecure mode, and if you have already upgraded the OMS, then run these commands, generate the health check report again, and then switch over:

```
$(OMS_HOME)/bin/emctl secure unlock -console
```

```
$(OMS_HOME)/bin/emctl secure unlock -upload
```

Caution: If your old Management Agent was running in secure (or unsecure) mode before backing up the Management Repository in case of the 2-System upgrade approach, then ensure that it continues to run in the same mode while you deploy and configure the new Management Agent for it. Otherwise, the ping test can fail due to a mismatch between the configuration stored in the repository and the actual configuration of the Management Agent.

- Verify the **Broken Targets** column, which indicates whether or not the deployed Oracle Management Agent 12c will be in a position to monitor all the targets that were monitored earlier by the old Management Agent. The numeric value you see in the column indicates the number of targets that cannot be monitored in the upgraded system.

If you see any value other than 0, then view the detailed report (as described in the next step) to see a list of broken targets and the reasons why they are broken.

- Verify the **Failed Metrics** column, which indicates whether or not the deployed and configured Oracle Management Agent 12c will be able to collect all the metrics in the upgraded Enterprise Manager system. The numeric value you see in the column indicates the number of metrics that have an issue.

If you see any value other than 0, then view the detailed report (as described in the next step) to see a list of failed metrics and the reasons for their failure.

-
- Verify the **Sign-Off User** column and the **User Verified** Column, which indicate whether or not the health report was signed off for a Management Agent. If you do not see any value in these columns, then formally sign off the report as described in Step (6).
5. If you want to view a detailed report, select the Management Agent for which you want to view a detailed report, and click **View Detailed Report**.
 6. After checking the report, click **Verify and Sign Off Report** to sign off. Ensure that the Management Agent for which you viewed a detailed report is selected.

Note:

- After you submit the operation, if you see the following error, then first run `root.sh` from the old Management Agent home, and then, resubmit this operation.

```
ERROR: NMO not setuid-root (Unix-only)
```

- If you see the following error, then verify the credentials entered in Step (10).

```
Local Authentication Failed...Attempt PAM authentication...PAM failed . . .
```

- If you were monitoring a SOA target in your earlier release of Enterprise Manager, then in the health report, you might see metric collection errors for the following metrics:

- Top SOA SQL Queries
- Dehydration Store Tables

As this stage, you can ignore these errors and proceed further. However, ensure that you provide the database credentials for this target as described in [Chapter 25](#).



Switching Over to Oracle Management Agent 12c

To switch over the existing, earlier release of Oracle Management Agents (Management Agent) to the newly deployed Management Agents, so that they can communicate with Enterprise Manager Cloud Control, follow these steps:

Note: Perform these steps in the Enterprise Manager Grid Control console of the earlier release.

Note: If you are upgrading using the 2-system upgrade approach or the 1-system upgrade approach on a different host, then DO NOT switch over the Management Agent (central agent) that was installed with the old Oracle Management Service (OMS).

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Agent Upgrade Steps section, from the table, click **Switch Agents**.
4. On the Switch Agents page, in the Provide Inputs section, do the following:
 - a. Enter a unique name for the switchover operation you are about to perform. The custom name you enter can be any intuitive name, and need not necessarily be in the same format as the default name.

For example, `Switch_Agents_Phase1_2010_12_23`

Note: The operation name you enter here is only a logical name and will be used for saving the details of the operation you are about to perform. After submitting this operation, if you want to track its status, then you can use the operation name.

- b. If you want to switch over the Management Agents for which you had previously performed a readiness check, then click the torch icon against **Load Agents from Previous Operations**, and select the operation you had submitted for performing the readiness check for those Management Agents, click **Go**.

Enterprise Manager Grid Control populates the table in the Search Agents section with a list of Management Agents that are associated with the operation you selected.

5. In the Search Agents section, search and add the Management Agents you want to switch over:
 - If you specified a switchover operation name as described in Step 4 (a), then search (or add) and select the deployed Management Agents that you want to switch over now. To understand how to search and add Management Agents, see [Appendix G](#).
 - If you selected an operation name as described in Step 4 (b), then review the Management Agents that are displayed based on the operation you selected.
6. After you add the Management Agents, select each of them from the **Select** column.
7. In the Agent Credentials section, retain the default selection, that is, **Use Oracle Home Preferred Credentials**, so that the preferred credentials stored in the Management Repository can be used for this job.

Note: Ensure that the preferred credentials were registered with the Enterprise Manager system using the Enterprise Manager Command Line Interface (EM CLI). For more information, see [Appendix F](#).

You can optionally override these preferred credentials. To do so, select **Override Oracle Home Preferred Credentials** and enter one set of credentials that can be used for all Oracle homes.

Note: Ensure that you use the same credentials that you used for the existing, earlier release of the Management Agent

8. Click **Submit**.

Points to Keep in Mind

Keep these points in mind:

- After you submit the operation, if you see the following error, then first run `root.sh` from the old Management Agent home, and then, resubmit this operation.

```
ERROR: NMO not setuid-root (Unix-only)
```
- If you see the following error, then verify the credentials entered in Step (10).

```
Local Authentication Failed...Attempt PAM authentication...PAM failed . . .
```
- When the operation is in progress, if a Management Agent being deployed and configured becomes unavailable for some reason, you may see the status *Suspended on Event*. Once the Management Agent becomes available, the status automatically changes to show the current state, and eventually gets switched over. This is an expected behavior.
- In the 2-System upgrade approach, all the old Management Agents you selected are switched over, and the upgraded Management Agents are started so that they can communicate with the upgraded OMS.

-
- **If you selected an old Management Agent that was installed with the old OMS, then that Management Agent is switched over but not started, and as a result, it continues to run.** This is an expected behavior because in the 2-System upgrade approach, your old OMS coexists with the new OMS for some time, and until the old OMS is decommissioned completely, the old Management Agent that was installed with it must continue to run.

When you are ready to decommission the old OMS, ensure that you manually stop this old Management Agent and start the upgraded (or switched over) Management Agent so that it can start communicating with the new OMS.

- In the 1-System upgrade approach, if you missed switching over any Management Agent and upgraded the OMS inadvertently, then you must manually switch over those Management Agents by first stopping the old Management Agents and then starting the new ones:

(a) Stop the old Management Agent home:

```
$<AGENT_HOME>/bin/emctl stop agent
```

(b) Start the deployed Oracle Management Agent 12c from its instance home:

```
$<AGENT_INSTANCE_DIR>/bin/emctl start agent
```

- Even after switching over a Management Agent, if the status shows that it is down, then manually start it:

```
$<AGENT_INSTANCE_DIR>/bin/emctl start agent
```

- While switching over a deployed Management Agent to the new Enterprise Manager system, the switchover job might fail at the *uploadAgent* step. If the step fails with that error, then do the following:

1. On the Management Agent host, run the following command:

```
cat /dev/null > access_log
```

2. From the Management Agent instance home, run the following command and verify if the upload operation succeeds. Repeat this command until the upload operation succeeds.

```
$<AGENT_INSTANCE_HOME>/bin/emctl upload agent
```

3. Once the upload operation succeeds, access the Upgrade Console from your Enterprise Manager Grid Control console, and in the Agent Upgrade Steps section, click **Switch Agents**.

4. On the Switch Agents page, select the Management Agent that had the error, and submit the switchover job again.



Part V

Upgrading Oracle Management Service and Oracle Management Repository

This part covers the following procedures:

- [Chapter 15, "Providing Repository Backup Details"](#)
- [Chapter 16, "Upgrading OMS and Repository in Graphical Mode"](#)
- [Chapter 17, "Upgrading OMS and Repository in Silent Mode"](#)
- [Chapter 18, "Installing Software Now and Upgrading Later in Graphical Mode"](#)
- [Chapter 19, "Installing Software Now and Upgrading Later in Silent Mode"](#)
- [Chapter 20, "Upgrading OMS and Repository for 1-System on Different Host Approach"](#)
- [Chapter 22, "Creating Link to Upgraded Oracle Management Repository"](#)
- [Chapter 21, "Upgrading Multi-OMS Environment"](#)

Providing Repository Backup Details

Note: Follow these instructions only if you are upgrading using the 2-System upgrade approach. Perform these steps in the Enterprise Manager Grid Control console of the earlier release.

To provide information on when you backed up your Oracle Management Repository, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Select Upgrade Type section, select **2-System**. For information about these upgrade approaches, see "Understanding Upgrade Approaches".

Enterprise Manager Grid Control refreshes the page and displays a table with a list of tasks you need to perform for the upgrade approach you selected.

4. In the OMS and Repository Upgrade Steps section, from the table, click **Provide Repository Backup Details**.
5. On the Provide Repository Backup Details page, provide the date and time when you backed up your Oracle Management Repository.
6. Click **Save**.



Upgrading OMS and Repository in Graphical Mode

This chapter describes how you can upgrade your existing Oracle Management Service (OMS) and Oracle Management Repository (Management Repository) in graphical mode using one of the upgrade approaches. In particular, this chapter covers the following:

- [Upgrading with 1-System Upgrade Approach in Graphical Mode](#)
- [Upgrading with 2-System Upgrade Approach in Graphical Mode](#)

Note: You can find the OMS and Management Agent entries in the `/etc/oragchomelist` file for all UNIX platforms except HPUNIX, HPia64, Solaris Sparc. On HPUNIX, HPia64, Solaris Sparc platforms, the entries are present in `/var/opt/oracle/oragchomelist`.

16.1 Upgrading with 1-System Upgrade Approach in Graphical Mode

Note: When you upgrade using the 1-System upgrade approach, the Enterprise Manager Cloud Control Installation Wizard does not install a Management Agent with the OMS it installs. The Management Agent is predeployed using the *Enterprise Manager 12c Upgrade Console*. This is an expected behavior.

To upgrade your existing OMS and Management Repository with 1-System upgrade approach in graphical mode, follow these steps:

1. Invoke the Enterprise Manager Cloud Control Installation Wizard on the host where your existing OMS is running.

```
<Software_Location>/runInstaller
```

In this command, `<Software_Location>` refers to the location where you have downloaded software kit.

Note: For information about the additional, advanced options you can pass while invoking the installer, refer to [Section 16.1.1](#).

Note: To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.

2. (Optional) On the My Oracle Support Details screen, enter your *My Oracle Support* credentials to enable Oracle Configuration Manager. If you do not want to enable Oracle Configuration Manager now, go to Step (3).

If the host from where you are running the installation wizard does not have a connection to the Internet, then enter only the e-mail address and leave the other fields blank. After you complete the installation, manually collect the configuration information and upload it to *My Oracle Support*.

3. Click **Next**.
4. On the Software Updates screen, select one of the following sources from where the software updates can be installed while the Enterprise Manager system gets upgraded. If you do not want to apply them now, then select **Skip**.
 - (Recommended) Select **Search for Updates**, and then, select **Local Directory** if you have already manually downloaded the software updates to an accessible local or remote location.

Enter the location where the updates are available, and click **Search for Updates**. To search the computer and select the location, click **Browse**. Once the search results appear with patch numbers and their details, click the patch number to view the ReadMe associated with that patch.

- If the updates have been downloaded to the default location, then select or enter the full path to the scratch path location. For example, if the scratch path location is `/scratch/OracleHomes` and if the software updates are available in `/scratch/OracleHomes/Updates`, then enter `/scratch/OracleHomes/Updates`.
- If the software updates have been downloaded to a custom location, then select or enter the full path to the custom location. For example, if the custom location is `/home/john` and if the software updates are available in `/home/john/Updates`, then enter `/home/john/Updates`.

- Select **Search for Updates**, and then, select **My Oracle Support** if you want the installer to connect to *My Oracle Support* and automatically download the updates from there.

Enter the My Oracle Support account user name and password, and click **Search for Updates**. Once the search results appear with patch numbers and their details, click the patch number to view the ReadMe associated with that patch

Note: If you choose to skip installing the software updates during installation by not providing the My Oracle Support credentials, you can always register the credentials later using the Enterprise Manager Cloud Control console and view the recommended security patches. To do so, log in to Enterprise Manager Cloud Control, and from the **Setup** menu, select **My Oracle Support**, and then, click **Set Credentials**. On the My Oracle Support Preferred Credentials page, enter the credentials and click **Apply**.

5. Click **Next**.
6. On the Prerequisite Checks screen, check the status of the prerequisite checks run by the installation wizard, and verify whether your environment meets all the minimum requirements for a successful upgrade.

The installation wizard runs the prerequisite checks automatically when you come to this screen. It checks for the required operating system patches, operating system packages, and so on.

The status of the prerequisite check can be either **Warning**, **Failed**, or **Succeeded**.

If some checks result in **Warning** or **Failed** status, then investigate and correct the problems before you proceed with the upgrade. The screen provides details on why the prerequisites failed and how you can resolve them. After you correct the problems, return to this screen and click **Rerun** to check the prerequisites again.

If you prefer to hide the successful checks and view only the ones with Warning or Failed status, then click **Hide Successful Checks**.

Note: Although Oracle recommends you to investigate and correct the problems, if you are compelled to proceed without resolving them, then select **Ignore** to ignore the warnings and failures. However, all package requirements must be met or fixed before proceeding any further. Otherwise, the upgrade might fail.

7. Click **Next**.
8. On the Install Types screen, do the following:
 - a. Select **Upgrade an Existing Enterprise Manager System**, and then, select **One System Upgrade**.
 - b. Select the OMS home you want to upgrade.
 - c. Validate or enter the middleware home.

Note:

- If you do not have Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24+ installed, then enter the absolute path to a directory where you want the installer to install them. For example, `/oracle/software/`. Ensure that the directory you enter does not contain any files or subdirectories.
 - If you have Oracle WebLogic Server and JDK already installed, then ensure that they are of the supported releases—Oracle WebLogic Server 11g Release 1 (10.3.5) and JDK 1.6 v24+. In this case, the installer detects them and displays the middleware home where they are installed. Validate the path to this middleware home.
 - If you want to install Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24 yourself, then follow the guidelines outlined in [Chapter 3](#).
-
-

9. Click **Next**.

10. On the Database Connection Details screen, enter the passwords for the SYS and SYSMAN user accounts of the database that houses the Management Repository for the selected OMS.

Note: Before you proceed to the next screen, stop all the associated OMSes. To do so, run the following command on each of the OMS hosts:

- If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0), then run this command from the OMS home:

```
$<OMS_HOME>/bin/emctl stop oms
```
 - If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0), then run this command from the OMS home:

```
$<OMS_HOME>/opmn/bin/opmnctl stopall
```
-

11. Click **Next**.

Note: If you encounter a Provisioning Archive Framework (PAF) prerequisite check error, then exit the installer, stop all the running and scheduled deployment procedures in your existing Enterprise Manager system, invoke the installer all over again, and retry the upgrade process.

12. On the Select Plug-Ins screen, select the optional plug-ins you want to install from the software kit (DVD, downloaded software) while upgrading the Enterprise Manager system.

The screen lists the mandatory plug-ins as well as the optional plug-ins. The grayed rows indicate the mandatory plug-ins that will be installed.

Note: The grayed rows might also include the plug-ins you installed while predeploying Oracle Management Agent 12c using the *Enterprise Manager 12c Upgrade Console*. However, if the grayed rows do not include the plug-ins you installed then, it means that those plug-ins are not available in the software kit. In that case, manually download those plug-ins to an accessible location and invoke the installer with an advanced option. For more information, see [Section 16.1.1](#) for the point on installing additional plug-ins.

13. Click **Next**.

14. Provide WebLogic Server Configuration Details

- If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0), then on the WebLogic Server Configuration Details screen, enter the credentials for the WebLogic Server user account and the Node Manager user account, and validate the path to the OMS instance base location.

Note: Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.

By default, the WebLogic Domain name is `GCDomain`, and the Node Manager name is `nodemanager`. These are non-editable fields. The installer uses this information for creating Oracle WebLogic Domain and other associated components such as the admin server, the managed server, and the node manager. A Node Manager enables you to start, shut down, or restart an Oracle WebLogic Server instance remotely, and is recommended for applications with high availability requirements.

- If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0), then on the Extend WebLogic Server Domain screen, validate the AdminServer host name and its port, and the WebLogic user name. Enter the WebLogic user account password for extending the existing Oracle WebLogic Server Domain to the upgraded release.
- If you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or from 11g Release 1 (11.1.0.1), then enter the host name and port of the AdminServer configured for the first OMS that you have already upgraded, and then, enter the credentials for the existing WebLogic Server user account.

15. Click **Next**.

16. On the Tablespace Location screen, validate the location where the data file (`mgmt_ad4j.dbf`) for JVM Diagnostics data tablespace can be stored. You can choose to edit it if you want. In that case, ensure that the path leads up to the file name. Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).

Note: This screen appears only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0).

17. Click **Next**.

18. Provide the port configuration details:

- If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0), then you will NOT see the Port Configuration Details screen because the ports used by the old OMS and the old Management Agent will be reused by the upgraded OMS and the Management Agent. Hence, go to Step (20).
- If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0), then on the Port Configuration Details screen, customize the ports to be used for various components.

Note:

- By default, this screen lists the default ports for all the core components. However, if you are upgrading an additional OMS, then the screen does not list the Admin Server HTTP SSL port because you will reuse the Admin Server configured for the first OMS.
 - If all the ports on this screen appear as -1, then it indicates that the installer is unable to bind the ports on the host. To resolve this issue, exit the installer, verify the host name and the IP configuration of this host (ensure that the IP address of the host is not being used by another host), restart the installer, and try again.
-

You can enter a free custom port that is either within or outside the port range recommended by Oracle.

To verify if a port is free, run the following command:

On Unix:

```
netstat -anp | grep <port no>
```

On Microsoft Windows:

```
netstat -an|findstr <port_no>
```

However, the custom port must be greater than 1024 and lesser than 65535. Alternatively, if you already have the ports predefined in a `staticports.ini` file and if you want to use those ports, then click **Import staticports.ini File** and select the file.

Note: If the `staticports.ini` file is passed during installation, then by default, the ports defined in the `staticports.ini` file are displayed. Otherwise, the first available port from the recommended range is displayed.

19. Click **Next**.
20. On the Review screen, review the details you have provided for the upgrade.
 - a. If you want to change the details, click **Back** repeatedly until you reach the screen where you want to make the changes.
 - b. After you verify the details, if you are satisfied, click **Install** to begin the upgrade.
21. On the Install Progress screen, view the overall progress (in percentage) of the upgrade operation and the status of each of the Configuration Assistants.

Note: If the OMS Configuration Assistant fails with an exception, particularly when you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0), then stop the AdminServer and try again. To stop the AdminServer, run the following command on each of the OMS hosts:

```
$<OMS_HOME>/bin/emctl stop oms -all
```

Note: If a Configuration Assistant fails, the installer stops and none of the subsequent Configuration Assistants are run until the issue related to the failed Configuration Assistant is resolved. In this case, diagnose the issue, resolve it, and then, click **Retry** on the Install Progress screen to rerun the Configuration Assistants starting from the Configuration Assistant that failed.

However, if you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home to rerun the Configuration Assistant in silent mode:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_
HOME=<absolute_path_to_OMS_home> MODE=perform
ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_
0.xml}
```

22. Once the software binaries are copied and configured, you are prompted to run the `allroot.sh` script. Open another window, log in as `root`, and manually run the scripts.

If you are installing on Microsoft Windows operating system, then you will NOT be prompted to run this script.

23. On the Finish screen, you should see information pertaining to the upgrade of Enterprise Manager. Review the information and click **Close** to exit the wizard.

16.1.1 Advanced Installer Options

The following are some additional, advanced options you can pass while invoking the installer:

- When you upgrade from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0), a new WebLogic domain named `GCDomain` is created by default. If you want to override this with a custom name, then invoke the installer with the `WLS_DOMAIN_NAME` option, and enter a unique custom name.

For example, if you want to use the custom name `EMDomain`, then run the following command:

```
./runInstaller WLS_DOMAIN_NAME=EMDomain
```

- By default, a Provisioning Advisor Framework (PAF) staging directory is created for copying the Software Library entities related to the deployment procedures. By default, this location is the scratch path location (`/tmp`). The location is used only for provisioning activities—entities are copied for a deployment procedure, and then, deleted once the deployment procedure ends.

If you want to override this location with a custom location, then invoke the installer with the `EM_STAGE_DIR` option, and enter a unique custom location.

For example,

```
./runInstaller EM_STAGE_DIR=/home/john/software/oracle/pafdir
```

- During upgrade, if you want to install some plug-ins that are not in the software kit (DVD, downloaded software), then follow these steps:
 1. Manually download the plug-ins from the following URL, and store them in an accessible location.

<http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html>

2. Invoke the installer with the following option, and pass the location where the plug-ins you want to install are available:

```
./runInstaller -pluginLocation <absolute_path_to_plugin_software_location>
```

This displays a list of plug-ins available in the software kit (DVD, downloaded software) as well as the plug-ins available in this custom location. You can choose the ones you want to install.

- After the upgrade operation ends successfully, the OMS and the Management Agent start automatically. If you do not want them to start automatically, then invoke the installer with `START_OMS` and `b_startAgent` options, and set them to `TRUE` or `FALSE` depending on what you want to control.

For example, if you do not want the Management Agent to start automatically, then run the following command:

```
./runInstaller START_OMS=TRUE b_startAgent=FALSE
```

To understand the limitations involved with this advanced option, see [Section 16.1.2](#).

16.1.2 Limitations

When you use `START_OMS` and `b_startAgent` as advanced options to control the way the OMS and the Management Agent start up automatically, sometimes the Management Agent and the host on which it was installed do not appear as targets in the Cloud Control console.

[Table 16-1](#) lists the different combinations of these advanced options, and describes the workaround to be followed for each combination:

Table 16-1 Advanced Options and Workarounds

Advanced Option	Workaround
<code>START_OMS=FALSE</code> <code>b_startAgent=FALSE</code>	<ol style="list-style-type: none"> 1. Start the OMS: <code>\$<OMS_HOME>/bin/emctl start oms</code> 2. Secure the Management Agent: <code>\$<AGENT_HOME>/bin/emctl secure agent</code> 3. Start the Management Agent: <code>\$<AGENT_HOME>/bin/emctl start agent</code> 4. Add the targets: <code>\$<AGENT_HOME>/bin/emctl config agent addinternaltargets</code> 5. Upload the targets: <code>\$<AGENT_HOME>/bin/emctl upload agent</code> 6. Manually configure the EMCLI tool in the <code>\$<ORACLE_HOME>/bin</code> directory. To do so, refer to the <i>Oracle Enterprise Manager Command Line Interface Guide</i>.

Table 16–1 (Cont.) Advanced Options and Workarounds

Advanced Option	Workaround
START_OMS=TRUE b_startAgent=FALSE	<ol style="list-style-type: none"> 1. Secure the Management Agent: <code style="padding-left: 20px;">\$<AGENT_HOME>/bin/emctl secure agent</code> 2. Start the Management Agent: <code style="padding-left: 20px;">\$<AGENT_HOME>/bin/emctl start agent</code> 3. Add the targets: <code style="padding-left: 20px;">\$<AGENT_HOME>/bin/emctl config agent addinternaltargets</code> 4. Upload the targets: <code style="padding-left: 20px;">\$<AGENT_HOME>/bin/emctl upload agent</code>
START_OMS=FALSE b_startAgent=TRUE	<ol style="list-style-type: none"> 1. Start the OMS: <code style="padding-left: 20px;">\$<OMS_HOME>/bin/emctl start oms</code> 2. Secure the Management Agent: <code style="padding-left: 20px;">\$<AGENT_HOME>/bin/emctl secure agent</code> 3. Add the targets: <code style="padding-left: 20px;">\$<AGENT_HOME>/bin/emctl config agent addinternaltargets</code> 4. Upload the targets: <code style="padding-left: 20px;">\$<AGENT_HOME>/bin/emctl upload agent</code> 5. Manually configure the EMCLI tool in the <code>\$<ORACLE_HOME>/bin</code> directory. To do so, refer to the <i>Oracle Enterprise Manager Command Line Interface Guide</i>.

16.2 Upgrading with 2-System Upgrade Approach in Graphical Mode

To upgrade your existing OMS and Management Repository with 2-System upgrade approach in graphical mode, follow these steps:

1. Invoke the Enterprise Manager Cloud Control Installation Wizard on the host where you plan to install Oracle Management Service 12c:

```
<Software_Location>/runInstaller [ALLOW_ONLY_SECURE_ACCESS_
TO_CONSOLE=FALSE LOCK_ORACLE_MANAGEMENT_SERVICE=FALSE]
```

In this command, `<Software_Location>` refers to the location where you have downloaded the software kit.

Note:

- For information about the additional, advanced options you can pass while invoking the installer, refer to [Section 16.1.1](#).
- To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.
- Ensure that the host on which you are invoking the installer matches with the host you entered in the *Enterpriser Manager 12c Upgrade Console*.

If you are invoking the installer on a different host, and if you choose to modify the host name in the *Enterpriser Manager 12c Upgrade Console*, then follow these steps:

1. Exit the installer.
2. Discard the backed up database.
3. Access the *Enterpriser Manager 12c Upgrade Console*:
 - (a) On the Identify Host and Port for New Enterprise Manager System page, change the host name. For instructions, see [Chapter 8](#).
 - (b) On the Deploy and Configure Agents page, reconfigure the Management Agents that have already been deployed. For instructions, see [Chapter 11](#).

Important: On the Deploy and Configure Agents page, in the Select Operation Type section, ensure that you deselect **Deploy Agent and Plug-In Software**.
4. Take a fresh backup of the database now.
5. Invoke the installer all over again, and retry the upgrade process.

- If the **Enterprise Manager Upload Http Port** and **Enterprise Manager Central Console Http Port** are unlocked in your existing Enterprise Manager system, then pass the optional arguments `ALLOW_ONLY_SECURE_ACCESS_TO_CONSOLE` and `LOCK_ORACLE_MANAGEMENT_SERVICE` while invoking the installer.

If you skip passing these arguments now, and if you want to unlock the ports later, then after upgrading the OMS, run these commands from the upgraded OMS home:

```
$<OMS_HOME>/bin/emctl secure unlock -console
$<OMS_HOME>/bin/emctl secure unlock -upload
```

2. (Optional) On the My Oracle Support Details screen, enter your *My Oracle Support* credentials to enable Oracle Configuration Manager. If you do not want to enable Oracle Configuration Manager now, go to Step (3).

If the host from where you are running the installation wizard does not have a connection to the Internet, then enter only the e-mail address and leave the other fields blank. After you complete the installation, manually collect the configuration information and upload it to *My Oracle Support*.

3. Click Next.

4. On the Software Updates screen, select one of the following sources from where the software updates can be installed while the installation of the Enterprise Manager system is in progress. If you do not want to apply them now, then select **Skip.**

- (Recommended) Select **Search for Updates**, and then, select **Local Directory** if you have already manually downloaded the software updates to an accessible local or remote location.

Enter the location where the updates are available, and click **Search for Updates**. To search the computer and select the location, click **Browse**. Once the search results appear with patch numbers and their details, click the patch number to view the ReadMe associated with that patch.

- If the updates have been downloaded to the default location, then select or enter the full path to the scratch path location. For example, if the scratch path location is `/scratch/OracleHomes` and if the software updates are available in `/scratch/OracleHomes/Updates`, then enter `/scratch/OracleHomes/Updates`.
- If the software updates have been downloaded to a custom location, then select or enter the full path to the custom location. For example, if the custom location is `/home/john` and if the software updates are available in `/home/john/Updates`, then enter `/home/john/Updates`.

- Select **Search for Updates**, and then, select **My Oracle Support** if you want the installer to connect to *My Oracle Support* and automatically download the updates from there.

Enter the My Oracle Support account user name and password, and click **Search for Updates**. Once the search results appear with patch numbers and their details, click the patch number to view the ReadMe associated with that patch

Note: If you choose to skip installing the software updates during installation by not providing the My Oracle Support credentials, you can always register the credentials later using the Enterprise Manager Cloud Control console and view the recommended security patches. To do so, log in to Enterprise Manager Cloud Control, and click **Preferences** from the top-right corner of the screen. On the General page, from the left menu bar, click **Preferred Credentials**. On the Preferred Credentials page, from the My Oracle Support Preferred Credentials section, click **Set Credentials**. On the My Oracle Support Preferred Credentials page, specify the credentials and click **Apply**.

5. Click Next.

If Enterprise Manager Cloud Control is the first Oracle product you are installing on the host that is running on UNIX operating system, then the Oracle Inventory screen appears. For details, see step (6). Otherwise, the Check Prerequisites screen appears. For details, see step (8).

If Enterprise Manager Cloud Control is the first Oracle product you are installing on the host that is running on Microsoft Windows operating system, then the Oracle Inventory screen does not appear. On Microsoft Windows, the following is the default inventory directory:

```
<system drive>\Program Files\Oracle\Inventory
```

6. On the Oracle Inventory screen, do the following. You will see this screen only if this turns out to be your first ever installation of an Oracle product on the host.
 - a. Enter the full path to a directory where the inventory files and directories can be placed.

Note:

- The central inventory location you enter must NOT be on a shared file system. If it is already on a shared file system, then switch over to a non-shared file system.
 - If this is the first Oracle product on the host, then the default central inventory location is `<home directory>/oraInventory`. However, if you already have some Oracle products on the host, then the central inventory location can be found in the `oraInst.loc` file. The `oraInst.loc` file is located in the `/etc` directory for Linux and AIX, and in the `/var/opt/oracle` directory for Solaris, HP-UX, and Tru64.
-
-

- b. Select the appropriate operating system group name that will own the Oracle inventory directories. The group that you select must have *write* permissions on the Oracle Inventory directories.
7. Click **Next**.
8. On the Prerequisite Checks screen, check the status of the prerequisite checks run by the installation wizard, and verify whether your environment meets all the minimum requirements for a successful upgrade.

The installation wizard runs the prerequisite checks automatically when you come to this screen. It checks for the required operating system patches, operating system packages, and so on.

The status of the prerequisite check can be either **Warning**, **Failed**, or **Succeeded**.

If some checks result in **Warning** or **Failed** status, then investigate and correct the problems before you proceed with the upgrade. The screen provides details on why the prerequisites failed and how you can resolve them. After you correct the problems, return to this screen and click **Rerun** to check the prerequisites again.

If you prefer to hide the successful checks and view only the ones with Warning or Failed status, then click **Hide Successful Checks**.

Note: Although Oracle recommends you to investigate and correct the problems, if you are compelled to proceed without resolving them, then select **Ignore** to ignore the warnings and failures. However, all package requirements must be met or fixed before proceeding any further. Otherwise, the upgrade might fail.

9. Click **Next**.
10. On the Install Types screen, do the following:
 - a. Select **Upgrade an Existing Enterprise Manager System**, and then, select **Two System Upgrade**.
 - b. Validate or enter the middleware home where you want to install the OMS and other core components.

Note:

- If you do not have Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24+ installed, then enter the absolute path to a directory where you want the installer to install them. For example, `/oracle/software/`. Ensure that the directory you enter does not contain any files or subdirectories.
 - If you have manually installed Oracle WebLogic Server and JDK, then ensure that they are of the supported releases—Oracle WebLogic Server 11g Release 1 (10.3.5) and JDK 1.6 v24+.

In this case, the installer detects them and displays the middleware home where they are installed. Validate the path to this middleware home.
 - If you want to install Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24 yourself, then follow the guidelines outlined in [Chapter 3](#).
-
-

11. Click **Next**.
12. On the Database Connection Details screen, enter the fully qualified name of the host where the backed up database resides, its listener port and its service name or system ID (SID), and the SYS and SYSMAN user account passwords.

Note: Oracle Real Application Cluster (Oracle RAC) nodes are referred to by their virtual IP (vip) names. The `service_name` parameter is used instead of the system identifier (SID) in `connect_data` mode, and failover is turned on. For more information, refer to *Oracle Database Net Services Administrator's Guide*.

The installer uses this information to connect to the backed up database for configuring the SYSMAN schema. SYSMAN schema holds most of the relational data used in managing Enterprise Manager Cloud Control.

13. Click **Next**.

Note:

- If you are connecting to an Oracle RAC database, and if you have entered the virtual IP address of one of its nodes, then the installation wizard prompts you with a Connection String dialog and requests you to update the connection string with information about the other nodes that are part of the cluster. Update the connection string and click **OK**. If you want to test the connection, click **Test Connection**.
 - Oracle Real Application Cluster (Oracle RAC) nodes are referred to by their virtual IP (vip) names. The `service_name` parameter is used instead of the system identifier (SID) in `connect_data` mode, and failover is turned on. For more information, refer to *Oracle Database Net Services Administrator's Guide*.
 - If you encounter a Provisioning Archive Framework (PAF) prerequisite check error, then do the following:
 - Exit the installer, run the following SQL command on the backed up database, invoke the installer all over again, and retry the upgrade process.

```
UPDATE MGMT_PAF_STATES
SET status = 6
WHERE state_type = 0
AND status IN (0, 1);
```
 - Exit the installer, discard the backed up database, stop all the running and scheduled deployment procedures in your existing Enterprise Manager system, take a fresh backup of the database now, invoke the installer all over again, and retry the upgrade process.
 - If you encounter any validation error, then follow these steps:
 1. Exit the installer.
 2. Discard the backed up database.
 3. Resolve the issue in the *Enterprise Manager 12c Upgrade Console*.
 4. Take a fresh backup of the database now.
 5. Invoke the installer all over again, and retry the upgrade process.
 - If you see a warning asking you to unlock the MGMT_VIEW user account and change the password, ignore it because the installer automatically unlocks it for you.
-

14. On the Select Plug-Ins screen, select the plug-ins you want to install while upgrading the Enterprise Manager system.

The screen lists the mandatory plug-ins as well as the optional plug-ins. The grayed rows indicate the mandatory plug-ins that will be installed.

Note: The grayed rows might also include the plug-ins you installed while predeploying Oracle Management Agent 12c using the *Enterprise Manager 12c Upgrade Console*. If the grayed rows do not include the plug-ins you installed then, it means that those plug-ins are not available in the software kit. In that case, manually download those plug-ins to an accessible location and invoke the installer with an advanced option. For more information, see [Section 16.1.1](#) for the point on installing additional plug-ins.

15. Click **Next**.

16. On the WebLogic Server Configuration Details screen, enter the credentials for the WebLogic Server user account and the Node Manager user account, and validate the path to the Oracle Management Service instance base location.

Note: Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.

By default, the WebLogic Domain name is `GCDomain`, and the Node Manager name is `nodemanager`. These are non-editable fields. The installer uses this information for creating Oracle WebLogic Domain and other associated components such as the admin server, the managed server, and the node manager. A Node Manager enables you to start, shut down, or restart an Oracle WebLogic Server instance remotely, and is recommended for applications with high availability requirements.

17. Click **Next**.

18. On the Old Repository Details screen, validate the connect string and enter the SYSMAN password of the old Management Repository.

The details are used to connect to the old Management Repository, check for accrued data, and seamlessly transfer it to the upgraded Management Repository. Accrued data refers to the data that was uploaded to the old Management Repository from the time it was backed up till the time it was upgraded.

Note: Typically, the connect string is prepopulated. However, if it is not prepopulated, then enter it in the following format:

- With SID

```
(DESCRIPTION= (ADDRESS_
LIST= (ADDRESS= (PROTOCOL=TCP) (HOST=<host_
name>) (PORT=<port>))) (CONNECT_DATA= (SID=<sid>)))
```

- With Service Name

```
(DESCRIPTION= (ADDRESS_
LIST= (ADDRESS= (PROTOCOL=TCP) (HOST=<host_
name>) (PORT=<port>))) (CONNECT_DATA= (SERVICE_
NAME=<service_name>)))
```

19. Click **Next**.

20. On the Tablespace Location screen, validate the location where the data file (mgmt_ad4j.dbf) for JVM Diagnostics data tablespace can be stored. You can choose to edit it if you want. In that case, ensure that the path leads up to the file name. Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).

Note: This screen appears only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0).

21. Click **Next**.

22. On the Port Configuration Details screen, customize the ports to be used for various components.

- Ensure that the ports you enter for **Enterprise Manager Upload Http Port** and **Enterprise Manager Upload Http SSL Port** match with the unsecure and secure ports you entered in the *Enterprise Manager 12c Upgrade Console*.

Note: If the ports mentioned in this screen are different from the ports you had entered in the *Enterprise Manager 12c Upgrade Console*, and if you decide to change the ports in the *Enterprise Manager 12c Upgrade Console*, then follow these steps:

1. Exit the installer.
 2. Discard the backed up database.
 3. Change the ports in the *Enterprise Manager 12c Upgrade Console*.
 4. Take a fresh backup of the database now.
 5. Invoke the installer all over again, and retry the upgrade process.
-
-

- For other components, you can enter a free custom port that is either within or outside the port range recommended by Oracle. However, the custom port must be greater than 1024 and lesser than 65535.

To verify if a port is free, run the following command:

On Unix:

```
netstat -anp | grep <port no>
```

On Microsoft Windows:

```
netstat -an|findstr <port_no>
```

- Alternatively, if you already have the ports predefined in a `staticports.ini` file and if you want to use those ports, then click **Import staticports.ini File** and select the file.

Note: If the `staticports.ini` file is passed during installation, then by default, the ports defined in the `staticports.ini` file are displayed. Otherwise, the first available port from the recommended range is displayed. If you do pass this file, then ensure that the ports you enter for **Enterprise Manager Upload Http Port** and **Enterprise Manager Upload Http SSL Port** match with the unsecure and secure ports you entered in the *Enterprise Manager 12c Upgrade Console*.

Note: If all the ports on this screen appear as -1, then it indicates that the installer is unable to bind the ports on the host. To resolve this issue, exit the installer, verify the host name and the IP configuration of this host (ensure that the IP address of the host is not being used by another host), restart the installer, and try again.

23. Click **Next**.
24. On the Review screen, review the details you provided for the selected installation type.
 - If you want to change the details, click **Back** repeatedly until you reach the screen where you want to make the changes.
 - After you verify the details, if you are satisfied, click **Install** to begin the installation process.
25. On the Install Progress screen, view the overall progress (in percentage) of the installation and the status of each of the Configuration Assistants. Configuration Assistants are run for configuring the installed components of Enterprise Manager Cloud Control.

Note: If a Configuration Assistant fails, the installer stops and none of the subsequent Configuration Assistants are run until the issue related to the failed Configuration Assistant is resolved. In this case, diagnose the issue, resolve it, and then, click **Retry** on the Install Progress screen to rerun the Configuration Assistants starting from the Configuration Assistant that failed.

However, if you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home to rerun the Configuration Assistant in silent mode:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_
HOME=<absolute_path_to_OMS_home> MODE=perform
ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_
0.xml}
```

26. Once the software binaries are copied and configured, you are prompted to run the `allroot.sh` script, and the `oraInstRoot.sh` script if this is the first Oracle product installation on the host. Open another window, log in as `root`, and manually run the scripts.

If you are installing on Microsoft Windows operating system, then you will NOT be prompted to run this script.

27. On the Finish screen, you should see information pertaining to the installation of Enterprise Manager. Review the information and click **Close** to exit the installation wizard.

For more information about this installation, refer to the following file available in the OMS home:

```
$<OMS_HOME>/install/setupinfo.txt
```

Upgrading OMS and Repository in Silent Mode

This chapter describes how you can upgrade your existing Oracle Management Service (OMS) and Oracle Management Repository (Management Repository) in silent mode using one of the upgrade approaches. In particular, this chapter covers the following:

- [Upgrading with 1-System Upgrade Approach in Silent Mode](#)
- [Upgrading with 2-System Upgrade Approach in Silent Mode](#)

Note: You can find the OMS and Management Agent entries in the `/etc/oragchomelist` file for all UNIX platforms except HPUNIX, HPia64, Solaris Sparc. On HPUNIX, HPia64, Solaris Sparc platforms, the entries are present in `/var/opt/oracle/oragchomelist`.

17.1 Upgrading with 1-System Upgrade Approach in Silent Mode

Note: When you upgrade using the 1-System upgrade approach, the Enterprise Manager Cloud Control Installation Wizard does not install a Management Agent with the OMS it installs. The Management Agent is predeployed using the *Enterprise Manager 12c Upgrade Console*. This is an expected behavior.

To upgrade your existing OMS and Management Repository with 1-System upgrade approach in silent mode, follow these steps:

1. Copy the following response file to an accessible location on your local host:

```
<Software_Location>/response/upgrade.rsp
```

In this command, `<Software_Location>` refers to the location where you have downloaded software kit.

2. Edit the response file and enter appropriate values for the variables described in [Table 17-1](#).

3. Invoke the installer:

```
./runInstaller -silent -responseFile <absolute_path>/upgrade.rsp
```

Note: For information about the additional, advanced options you can pass while invoking the installer, refer to [Section 17.1.1](#).

Note: To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.

17.1.1 Using Advanced Installer Options

The following are some additional, advanced options you can pass while invoking the installer:

- If you are upgrading on a host that has multiple host names (for example, virtual host), then pass the fully qualified host name using the `ORACLE_HOSTNAME` argument while invoking the installer.

For example:

```
./runInstaller ORACLE_HOSTNAME=example.com -silent
-responseFile <absolute_path>/upgrade.rsp
```

- After the installation ends successfully, the OMS and the Management Agent start automatically. If you do not want them to start automatically, then invoke the installer with `START_OMS` and `b_startAgent` options, and set them to `TRUE` or `FALSE` depending on what you want to control.

For example, if you do not want the Management Agent to start automatically, then run the following command:

```
./runInstaller START_OMS=TRUE b_startAgent=FALSE -silent
-responseFile <absolute_path>/upgrade.rsp
```

To understand the limitations involved with this advanced option, see [Section 16.1.2](#).

17.1.2 Editing Response File for Upgrading with 1-System Upgrade Approach in Silent Mode

[Table 17-1](#) describes what variables you must update and how you must update them in the `upgrade.rsp` response file for upgrading your OMS and Management Repository.

Table 17-1 *Editing Response File for Upgrading with 1-System Upgrade Approach in Graphical Mode*

Parameter	Description
UNIX_GROUP_NAME	Enter the name of the UNIX group you belong to. For example, "dba"
INVENTORY_LOCATION	Enter the absolute path to the Central Inventory. For example, /scratch/oracle/oraInventory

Table 17-1 (Cont.) Editing Response File for Upgrading with 1-System Upgrade Approach in Graphical Mode

Parameter	Description
SECURITY_UPDATES_VIA_MYORACLESUPPORT	<ul style="list-style-type: none"> ■ Enter TRUE if you want to download and install security updates. Then, enter the credentials for the following variables: MYORACLESUPPORT_USERNAME MYORACLESUPPORT_PASSWORD ■ Enter FALSE if you do not want to download and install security updates:
DECLINE_SECURITY_UPDATES	<ul style="list-style-type: none"> ■ Enter TRUE if you want to decline the security updates. In this case, you should have entered FALSE for SECURITY_UPDATES_VIA_MYORACLESUPPORT. ■ Enter FALSE if you do not want to decline the security updates. In this case, you should have entered TRUE for SECURITY_UPDATES_VIA_MYORACLESUPPORT.
INSTALL_UPDATES_SELECTION	<p>By default, this variable is set to "skip" indicating that the software updates will not be installed during installation.</p> <ul style="list-style-type: none"> ■ If you want to install the software updates from My Oracle Support, then set this variable to "download". Then, enter the credentials for the following parameters: MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES ■ If you want to install the software updates from a staged location, then set this variable to "staged". Then, for the STAGE_LOCATION parameter, enter the absolute path, which leads to the Updates directory, where the software updates are available.
ORACLE_MIDDLEWARE_HOME_LOCATION	<p>Enter the location where you want the installer to install Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24.</p> <p>For example, u01/app/Oracle/Middleware.</p> <p>Ensure that the middleware location has <i>write</i> permission.</p> <p>If you have already installed them manually, then enter the location where you have installed them.</p> <p>Note: Ensure that the middleware home you enter here is used only for Enterprise Manager Cloud Control. Ensure that no other Oracle Fusion Middleware products or components are installed in the same middleware home.</p>
ORACLE_INSTANCE_HOME_LOCATION	<p>By default, <code>gc_inst</code> is considered as the OMS Instance Base directory for storing all OMS-related configuration files, and the by default, it is created in the middleware home. If you want to accept the default location and the directory name, then skip this variable. However, if you want to have a custom location and a custom directory name, then enter the absolute path to the custom location leading up to the custom directory name.</p>
OLD_BASE_DIR	Enter the base directory of the OMS you want to upgrade.

Table 17–1 (Cont.) Editing Response File for Upgrading with 1-System Upgrade Approach in Graphical Mode

Parameter	Description
ONE_SYSTEM	By default, this variable is set to TRUE. Retain the default setting.
WLS_ADMIN_SERVER_USERNAME	<p><i>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</i></p> <p>By default, <code>wellogic</code> is the name assigned to the default user account that is created for the Oracle WebLogic Domain. If you want to accept the default name, then blank. However, if you want to have a custom name, then enter the name of your choice.</p> <p>Important: If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1) or if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1), then comment out this variable.</p>
WLS_ADMIN_SERVER_PASSWORD	<p><i>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</i></p> <p>Enter a password for the WebLogic user account.</p> <p>Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.</p> <p>Important: If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1) or if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1), then comment out this variable.</p>
WLS_ADMIN_SERVER_CONFIRM_PASSWORD	<p><i>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</i></p> <p>Confirm the password for the WebLogic user account.</p> <p>Important: If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1) or if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1), then comment out this variable.</p>
NODE_MANAGER_PASSWORD	<p><i>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</i></p> <p>By default, <code>nodemanager</code> is the name assigned to the default user account that is created for the node manager. Enter a password for this node manager user account.</p> <p>Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.</p> <p>Important: If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1) or if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1), then comment out this variable.</p>

Table 17–1 (Cont.) Editing Response File for Upgrading with 1-System Upgrade Approach in Graphical Mode

Parameter	Description
NODE_MANAGER_CONFIRM_PASSWORD	<p>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</p> <p>Confirm the password for the node manager user account.</p> <p>Important: If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1) or if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1), then comment out this variable.</p>
WLS_ADMIN_SERVER_PASSWORD	<p>(Applicable only if you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1))</p> <p>Enter the password for the WebLogic user account you had created for Enterprise Manager 11g Grid Control Release 1 (11.1.0.1).</p> <p>Important: If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1), then comment out this variable.</p>
ADMIN_SERVER_HOSTNAME	<p>(Applicable only if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1))</p> <p>Enter the host name of the AdminServer that is configured for the first OMS.</p> <p>Important: If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), then comment out this variable.</p>
ADMIN_SERVER_PORT	<p>(Applicable only if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1))</p> <p>Enter the port of the AdminServer that is configured for the first OMS.</p> <p>Important: If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), then comment out this variable.</p>
WLS_ADMIN_SERVER_USERNAME	<p>(Applicable only if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1))</p> <p>By default, <code>weblogic</code> is the name assigned to the default user account that is created for the Oracle WebLogic Domain. If you want to accept the default name, then blank. However, if you want to have a custom name, then enter the name of your choice.</p> <p>Important: If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), then comment out this variable.</p>

Table 17–1 (Cont.) Editing Response File for Upgrading with 1-System Upgrade Approach in Graphical Mode

Parameter	Description
WLS_ADMIN_SERVER_PASSWORD	<p>(Applicable only if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1))</p> <p>Enter a password for the WebLogic user account.</p> <p>Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.</p> <p>Important: If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), then comment out this variable.</p>
JVM_DIAGNOSTICS_TABLESPACE_LOCATION	<p>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</p> <p>Enter the absolute path to a location where the data file (mgmt_ad4j.dbf) for JVM Diagnostics data tablespace can be stored. Ensure that the specified path leads up to the file name.</p> <p>For example, /home/john/oradata/mgmt_ad4j.dbf</p> <p>Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).</p>
SYS_PASSWORD	Enter the SYS user account's password.
SYSMAN_PASSWORD	Enter the SYSMAN user account's password.
STATIC_PORTS_FILE	<ul style="list-style-type: none"> ▪ If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0), then skip this parameter because the same ports are carried over to Enterprise Manager Cloud Control. ▪ If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0), then enter the absolute path to the staticports.ini file that contains ONLY the following ports: <ul style="list-style-type: none"> Admin Server Http SSL Port Managed Server Http Port Managed Server Http SSL Port Node Manager Http SSL Port <p>You must skip the other ports in the staticports.ini file because the ports used in the earlier release will be carried over to Enterprise Manager Cloud Control.</p> <p>The staticports.ini file is available in the following location of the software kit (DVD, downloaded software): <software_kit>/response/staticports.ini</p>

Table 17–1 (Cont.) Editing Response File for Upgrading with 1-System Upgrade Approach in Graphical Mode

Parameter	Description
PLUGIN_SELECTION	<p>By default, mandatory plug-ins such as Oracle Database Management Plug-In, Oracle Fusion Middleware Management Plug-In, Oracle My Oracle Support Management Plug-In, and Oracle Exadata Management Plug-In get automatically installed when you upgrade your Enterprise Manager.</p> <p>However, if you want to install any of the other optional plug-ins that are available in the software kit (DVD or downloaded software), then enter the names of those plug-ins for this variable.</p> <p>For example,</p> <pre>PLUGIN_SELECTION={ "oracle.sysman.empa" , "oracle.sysman.vt" }</pre> <p>If you want to install any plug-in that is not available in the software kit, then do the following:</p> <ol style="list-style-type: none"> 1. Manually download the plug-ins from the following URL, and store them in an accessible location. <p>http://www.oracle.com/technetwork/oem/g rid-control/downloads/oem-upgrade-console-502238.html</p> 2. Update this variable (PLUGIN_SELECTION) to the names of those plug-ins you downloaded. 3. Invoke the installer with the following option, and pass the location where you downloaded the plug-ins: <pre>./runInstaller -pluginLocation <absolute_path_to_plugin_software_location></pre>

17.2 Upgrading with 2-System Upgrade Approach in Silent Mode

To upgrade your existing OMS and Management Repository using 2-System upgrade approach in silent mode, follow these steps:

1. Copy the following response file to an accessible location on your local host:

```
<Software_Location>/response/upgrade.rsp
```

In this command, <Software_Location> refers to the location where you have downloaded the software kit.

2. Edit the response file and enter appropriate values for the variables described in [Table 17–2](#).
3. Invoke the installer:
 - If this is the first Oracle product you are installing on the host, then run the following command on the host where you plan to install Oracle Management Service 12c:

```
./runInstaller -silent -responseFile <absolute_path>/upgrade.rsp [-invPtrLoc <absolute_path_to_inventory_directory>] -staticPortsIniFile <absolute_path_to_staticports.ini_file> [ALLOW_ONLY_SECURE_ACCESS_TO_CONSOLE=FALSE LOCK_ORACLE_MANAGEMENT_SERVICE=FALSE]
```

Note: The central inventory location you enter must NOT be on a shared file system.

- Otherwise, run the following command:

```
./runInstaller -silent -responseFile <absolute_path>/upgrade.rsp -staticPortsIniFile <absolute_path_to_file>
```

Note: For information about the additional, advanced options you can pass while invoking the installer, refer to [Section 17.1.1](#).

To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.

Note:

- Ensure that the host on which you are invoking the installer matches with the host you entered in the *Enterpriser Manager 12c Upgrade Console*.

If you are invoking the installer on a different host, and if you choose to modify the host name in the *Enterpriser Manager 12c Upgrade Console*, then follow these steps:

1. Exit the installer.
2. Discard the backed up database.
3. Access the *Enterpriser Manager 12c Upgrade Console*, and change the host name in the Identify Host and Port for New Enterprise Manager System page.
4. Take a fresh backup of the database now.
5. Invoke the installer all over again, and retry the upgrade process.

In this case, you must ensure that all the Management Agents, which were already deployed and configured through the *Enterpriser Manager 12c Upgrade Console* before upgrading the OMS, are reconfigured with the new host name.

- In the `staticports.ini` file, ensure that the ports you enter for **Enterprise Manager Upload Http Port** and **Enterprise Manager Upload Http SSL Port** match with the unsecure and secure ports you entered in the *Enterprise Manager 12c Upgrade Console*.

If you decide to change the ports in the *Enterprise Manager 12c Upgrade Console* instead, then follow these steps:

1. Exit the installer.
2. Discard the backed up database.
3. Change the ports in the *Enterprise Manager 12c Upgrade Console*.
4. Take a fresh backup of the database now.
5. Invoke the installer all over again, and retry the upgrade process.

Note: If the **Enterprise Manager Upload Http Port** and **Enterprise Manager Central Console Http Port** are unlocked in your existing Enterprise Manager system, then pass the arguments `ALLOW_ONLY_SECURE_ACCESS_TO_CONSOLE` and `LOCK_ORACLE_MANAGEMENT_SERVICE` while invoking the installer.

If you skip passing these arguments now, and if you want to unlock the ports later, then after upgrading the OMS, run these commands from the upgraded OMS home:

```
$<OMS_HOME>/bin/emctl secure unlock -console
```

```
$<OMS_HOME>/bin/emctl secure unlock -upload
```

17.2.1 Editing Response File for Upgrading with 2-System Upgrade Approach in Silent Mode

Table 17–2 describes what variables you must update and how you must update them in the `upgrade.rsp` response file for upgrading your OMS and Management Repository.

Table 17–2 *Editing Response File for Upgrading with 2-System Upgrade Approach in Silent Mode*

Parameter	Description
UNIX_GROUP_NAME	Enter the name of the UNIX group you belong to. For example, "dba"
INVENTORY_LOCATION	Enter the absolute path to the Central Inventory. For example, /scratch/oracle/oraInventory
SECURITY_UPDATES_VIA_MYORACLESUPPORT	<ul style="list-style-type: none"> ■ Enter TRUE if you want to download and install security updates. Then, enter the credentials for the following variables: MYORACLESUPPORT_USERNAME MYORACLESUPPORT_PASSWORD ■ Enter FALSE if you do not want to download and install security updates:
DECLINE_SECURITY_UPDATES	<ul style="list-style-type: none"> ■ Enter TRUE if you want to decline the security updates. In this case, you should have entered <code>False</code> for SECURITY_UPDATES_VIA_MYORACLESUPPORT. ■ Enter FALSE if you do not want to decline the security updates. In this case, you should have entered <code>TRUE</code> for SECURITY_UPDATES_VIA_MYORACLESUPPORT.
INSTALL_UPDATES_SELECTION	<p>By default, this variable is set to "skip" indicating that the software updates will not be installed during installation.</p> <ul style="list-style-type: none"> ■ If you want to install the software updates from My Oracle Support, then set this variable to "download". Then, enter the credentials for the following parameters: MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES ■ If you want to install the software updates from a staged location, then set this variable to "staged". Then, for the <code>STAGE_LOCATION</code> parameter, enter the absolute path, which leads to the <code>Updates</code> directory, where the software updates are available.

Table 17–2 (Cont.) Editing Response File for Upgrading with 2-System Upgrade Approach in Silent Mode

Parameter	Description
ORACLE_MIDDLEWARE_HOME_LOCATION	<p>Enter the location where you want the installer to install Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24.</p> <p>For example, <code>u01/app/Oracle/Middleware</code>.</p> <p>Ensure that the middleware location has <i>write</i> permission. Enter that this location is not an NFS-mounted location.</p> <p>If you have already installed them manually, then enter the location where you have installed them.</p> <p>Note: Ensure that the middleware home you enter here is used only for Enterprise Manager Cloud Control. Ensure that no other Oracle Fusion Middleware products or components are installed in the same middleware home.</p>
ORACLE_INSTANCE_HOME_LOCATION	<p>By default, <code>gc_inst</code> is considered as the OMS Instance Base directory for storing all OMS-related configuration files, and the by default, it is created in the middleware home. If you want to accept the default location and the directory name, then skip this variable. However, if you want to have a custom location and a custom directory name, then enter the absolute path to the custom location leading up to the custom directory name.</p> <p>Note: If you have entered an NFS-mounted drive for the <code>ORACLE_MIDDLEWARE_HOME_LOCATION</code> parameter, then ensure that the location you enter for this parameter is a non-NFS-mounted location.</p>
ONE_SYSTEM	By default, this variable is set to <code>TRUE</code> . Change the value to <code>FALSE</code> .
OLD_DATABASE_CONNECTION_DESCRIPTION	<p>Enter the connect string in the following format to connect to the old Management Repository.</p> <ul style="list-style-type: none"> ■ With SID <pre>(DESCRIPTION= (ADDRESS_ LIST= (ADDRESS= (PROTOCOL=TCP) (HOST=<host_ _name>) (PORT=<port>))) (CONNECT_ DATA= (SID=<sid>)))</pre> ■ With Service Name <pre>(DESCRIPTION= (ADDRESS_ LIST= (ADDRESS= (PROTOCOL=TCP) (HOST=<host_ _name>) (PORT=<port>))) (CONNECT_ DATA= (SERVICE_NAME=<service_name>)))</pre> <p>The connect string is used to connect to the old Management Repository, check for accrued data, and seamlessly transfer it to the upgraded Management Repository. Accrued data refers to the data that was uploaded to the old Management Repository from the time it was backed up till the time it was upgraded.</p>
OLD_DATABASE_SYSMAN_PASSWORD	Enter the SYSMAN password of the old Management Repository.
WLS_ADMIN_SERVER_USERNAME	By default, <code>weblogic</code> is the name assigned to the default user account that is created for the Oracle WebLogic Domain. If you want to accept the default name, then blank. However, if you want to have a custom name, then enter the name of your choice.

Table 17-2 (Cont.) Editing Response File for Upgrading with 2-System Upgrade Approach in Silent Mode

Parameter	Description
WLS_ADMIN_SERVER_PASSWORD	Enter a password for the WebLogic user account. Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.
WLS_ADMIN_SERVER_CONFIRM_PASSWORD	Confirm the password for the WebLogic user account.
NODE_MANAGER_PASSWORD	By default, nodemanager is the name assigned to the default user account that is created for the node manager. Enter a password for this node manager user account. Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.
NODE_MANAGER_CONFIRM_PASSWORD	Confirm the password for the node manager user account.
WLS_ADMIN_SERVER_PASSWORD	Comment out this variable.
ADMIN_SERVER_HOSTNAME	Comment out this variable.
ADMIN_SERVER_PORT	Comment out this variable.
WLS_ADMIN_SERVER_USERNAME	Comment out this variable.
WLS_ADMIN_SERVER_PASSWORD	Comment out this variable.
JVM_DIAGNOSTICS_TABLESPACE_LOCATION	(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5)) Enter the absolute path to a location where the data file (mgmt_ad4j.dbf) for JVM Diagnostics data tablespace can be stored. Ensure that the specified path leads up to the file name. For example, /home/john/oradata/mgmt_ad4j.dbf Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).

Table 17-2 (Cont.) Editing Response File for Upgrading with 2-System Upgrade Approach in Silent Mode

Parameter	Description
DATABASE_HOSTNAME	<p>Enter the fully qualified name of the host where the existing database resides.</p> <p>For example, <code>example.com</code></p> <p>If you are connecting to an Oracle RAC Database, and if the nodes have virtual host names, then enter the virtual host name of one of its nodes.</p> <p>The connection to the database is established with a connect string that is formed using only this virtual host name, and the installation ends successfully.</p> <p>However, if you want to update the connect string with other nodes of the cluster, then after the installation, do the following:</p> <ol style="list-style-type: none"> 1. Open the following file: <code><OMS_Instance_Home>/em/EMGC_OMS#/emgc.properties</code> 2. Enter the other nodes for the variable <code>EM_RESPOS_CONNECTDESCRIPTOR</code>.
LISTENER_PORT	<p>Enter the listener port to connect to the existing database.</p> <p>For example, <code>1532</code></p>
SERVICENAME_OR_SID	<p>Enter the service name or the system ID (SID) of the existing database.</p> <p>For example, <code>orcl</code></p>
SYS_PASSWORD	Enter the SYS user account's password.
SYSMAN_PASSWORD	Enter the SYSMAN user account's password.
STATIC_PORTS_FILE	<ul style="list-style-type: none"> ■ The default ports are honored. If you want to accept the default ports, then skip this field. <p>For information about the default ports, see the <i>Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide</i>.</p> <ul style="list-style-type: none"> ■ If you want to use custom ports, then enter the absolute path to the <code>staticports.ini</code> file that lists the custom ports to be used for the installation. <p>The <code>staticports.ini</code> file is available in the following location of the software kit (DVD, downloaded software): <code><software_kit>/response/staticports.ini</code></p>

Table 17-2 (Cont.) Editing Response File for Upgrading with 2-System Upgrade Approach in Silent Mode

Parameter	Description
<p>PLUGIN_SELECTION</p>	<p>By default, mandatory plug-ins such as Oracle Database Management Plug-In, Oracle Fusion Middleware Management Plug-In, Oracle My Oracle Support Management Plug-In, and Oracle Exadata Management Plug-In get automatically installed when you upgrade your Enterprise Manager.</p> <p>However, if you want to install any of the other optional plug-ins that are available in the software kit (DVD or downloaded software), then enter the names of those plug-ins for this variable.</p> <p>For example,</p> <pre> PLUGIN_SELECTION={ "oracle.sysman.empa" , "oracle.sysman.vt" } </pre> <p>If you want to install any plug-in that is not available in the software kit, then do the following:</p> <ol style="list-style-type: none"> 1. Manually download the plug-ins from the following URL, and store them in an accessible location. <p>http://www.oracle.com/technetwork/oem/guid-control/downloads/oem-upgrade-console-502238.html</p> 2. Update this variable (PLUGIN_SELECTION) to the names of those plug-ins you downloaded. 3. Invoke the installer with the following option, and pass the location where you downloaded the plug-ins: <pre> ./runInstaller -pluginLocation <absolute_path_to_plugin_software_location> </pre>

Installing Software Now and Upgrading Later in Graphical Mode

This chapter explains how you can install only the software binaries of Enterprise Manager Cloud Control in graphical mode at one point, and upgrade them at a later point.

This is called the *software-only* mode, and it enables you to divide the upgrade process into two phases, mainly the installation phase and the upgrade phase.

Understandably, the installation phase takes less time compared to the upgrade phase because the installation phase involves only copying of binaries. In addition, this approach helps you plan your upgrade according to the time and priorities you have.

While you can perform this software-only upgrade in graphical and silent mode, this chapter describes how you perform it in graphical mode.

This chapter covers the following:

- [Upgrading in Software-Only Mode with 1-System Upgrade Approach](#)
- [Upgrading in Software-Only Mode with 2-System Upgrade Approach](#)

Note: You can find the OMS and Management Agent entries in the `/etc/oragchomelist` file for all UNIX platforms except HPUNIX, HPia64, Solaris Sparc. On HPUNIX, HPia64, Solaris Sparc platforms, the entries are present in `/var/opt/oracle/oragchomelist`.

18.1 Upgrading in Software-Only Mode with 1-System Upgrade Approach

This section describes how you can upgrade your OMS and Management Repository in software-only mode with 1-System upgrade approach. In particular, this section covers the following:

- [Installing Software Binaries](#)
- [Running `allroot.sh` Script](#)
- [Configuring and Upgrading](#)

18.1.1 Installing Software Binaries

To install the software binaries of Enterprise Manager Cloud Control, follow these steps:

1. Invoke the Enterprise Manager Cloud Control installer on the host where your existing OMS is running.

```
<Software_Location>/runInstaller [-invPtrLoc <absolute_path_to_oraInst.loc>]
```

Note:

- In this command, <Software_Location> refers to the location where you have downloaded software kit.
 - To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.
 - For information about the additional, advanced options you can pass while invoking the installer, refer to [Section 16.1.1](#).
 - The central inventory location you enter must NOT be on a shared file system.
-
-

2. (Optional) On the My Oracle Support Details screen, enter your *My Oracle Support* credentials to enable Oracle Configuration Manager. If you do not want to enable Oracle Configuration Manager now, go to Step (3).

If the host from where you are running the installation wizard does not have a connection to the Internet, then enter only the e-mail address and leave the other fields blank. After you complete the installation, manually collect the configuration information and upload it to *My Oracle Support*.

3. Click **Next**.
4. On the Software Updates screen, select one of the following sources from where the software updates can be installed while the Enterprise Manager system gets upgraded. If you do not want to apply them now, then select **Skip**.
 - (Recommended) Select **Search for Updates**, and then, select **Local Directory** if you have already manually downloaded the software updates to an accessible local or remote location.

Enter the location where the updates are available, and click **Search for Updates**. To search the computer and select the location, click **Browse**. Once the search results appear with patch numbers and their details, click the patch number to view the ReadMe associated with that patch.

- If the updates have been downloaded to the default location, then select or enter the full path to the scratch path location. For example, if the scratch path location is `/scratch/OracleHomes` and if the software updates are available in `/scratch/OracleHomes/Updates`, then enter `/scratch/OracleHomes/Updates`.
- If the software updates have been downloaded to a custom location, then select or enter the full path to the custom location. For example, if the custom location is `/home/john` and if the software updates are available in `/home/john/Updates`, then enter `/home/john/Updates`.

- Select **Search for Updates**, and then, select **My Oracle Support** if you want the installer to connect to *My Oracle Support* and automatically download the updates from there.

Enter the My Oracle Support account user name and password, and click **Search for Updates**. Once the search results appear with patch numbers and

their details, click the patch number to view the ReadMe associated with that patch

Note: If you choose to skip installing the software updates during installation by not providing the My Oracle Support credentials, you can always register the credentials later using the Enterprise Manager Cloud Control console and view the recommended security patches. To do so, log in to Enterprise Manager Cloud Control, and from the **Setup** menu, select **My Oracle Support**, and then, click **Set Credentials**. On the My Oracle Support Preferred Credentials page, enter the credentials and click **Apply**.

5. Click **Next**.
6. On the Prerequisite Checks screen, check the status of the prerequisite checks run by the installation wizard, and verify whether your environment meets all the minimum requirements for a successful upgrade.

The installation wizard runs the prerequisite checks automatically when you come to this screen. It checks for the required operating system patches, operating system packages, and so on.

The status of the prerequisite check can be either **Warning**, **Failed**, or **Succeeded**.

If some checks result in **Warning** or **Failed** status, then investigate and correct the problems before you proceed with the upgrade. The screen provides details on why the prerequisites failed and how you can resolve them. After you correct the problems, return to this screen and click **Rerun** to check the prerequisites again.

If you prefer to hide the successful checks and view only the ones with Warning or Failed status, then click **Hide Successful Checks**.

Note: Although Oracle recommends you to investigate and correct the problems, if you are compelled to proceed without resolving them, then select **Ignore** to ignore the warnings and failures. However, all package requirements must be met or fixed before proceeding any further. Otherwise, the upgrade might fail.

7. Click **Next**.
8. On the Install Types screen, do the following:
 - a. Select **Install software only**.
 - b. Validate or enter the middleware home where you want to install the OMS and other core components.

Note:

- If you do not have Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24+ installed, then enter the absolute path to a directory where you want the installer to install them. For example, `/oracle/software/`. Ensure that the directory you enter does not contain any files or subdirectories.
 - If you have Oracle WebLogic Server and JDK already installed, then ensure that they are of the supported releases—Oracle WebLogic Server 11g Release 1 (10.3.5) and JDK 1.6 v24+. In this case, the installer detects them and displays the middleware home where they are installed. Validate the path to this middleware home.
 - If you want to install Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24 yourself, then follow the guidelines outlined in [Chapter 3](#).
-
-

9. Click Next.

- 10.** On the Select Plug-Ins screen, select the optional plug-ins you want to install from the software kit while installing the software binaries. The screen lists the mandatory plug-ins as well as the optional plug-ins. The grayed rows indicate the mandatory plug-ins that will be installed.

Note: If you want to install a plug-in that is not available in the software kit, then refer to the point about installing additional plug-ins in [Section 16.1.1](#).

11. Click Next.

- 12.** On the Review screen, review the details you provided for the selected installation type.
- If you want to change the details, click **Back** repeatedly until you reach the screen where you want to make the changes.
 - After you verify the details, if you are satisfied, click **Install** to begin the installation process.
- 13.** On the Install Progress screen, view the overall progress (in percentage) of the installation.
- 14.** On the Finish screen, you should see information pertaining to the installation of Enterprise Manager. Review the information and click **Close** to exit the installation wizard.
- 15.** Deinstall the Management Agent. For instructions, refer to the chapter on deinstalling a Management Agent in the *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.

Note: The Management Agent installed with the OMS is not required because you already have the Management Agent predeployed by the *Enterprise Manager 12c Upgrade Console*.

18.1.2 Running allroot.sh Script

(For UNIX Only) After you install the software binaries, log in as a *root* user in a new terminal and run the `allroot.sh` script from the OMS home:

```
$<OMS_HOME>/allroot.sh
```

18.1.3 Configuring and Upgrading

To configure the software binaries of Enterprise Manager Cloud Control, follow these steps:

1. Invoke the installation wizard by running the following script:

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh  
[-invPtrLoc <absolute_path_to_oraInst.loc>]
```

Note:

- While installing the software binaries as described in [Section 18.1.1](#), if you had passed the argument `-invPtrLoc`, then pass the same argument here as well.
 - For information about the additional, advanced options you can pass while invoking the script, refer to [Section 18.1.3.1](#).
-
-

2. On the Install Types screen, do the following:
 - a. Select **Upgrade an Existing Enterprise Manager System**, and then, select **One System Upgrade**.
 - b. Select the OMS home you want to upgrade.
3. Click **Next**.
4. On the Database Connection Details screen, enter the passwords for the SYS and SYSMAN user accounts of the database that houses the Management Repository for the selected OMS.

Note: Before you proceed to the next screen, stop all the associated OMSes. To do so, run the following command on each of the OMS hosts:

- If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0), then run this command from the OMS home:

```
$<OMS_HOME>/bin/emctl stop oms
```
 - If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0), then run this command from the OMS home:

```
$<OMS_HOME>/opmn/bin/opmnctl stopall
```
-
-

5. Click **Next**.

Note: If you see an error about missing plug-ins, then manually download those plug-ins (opar files) to an accessible location, and invoke the installer once again in the following way to install the software binaries of the downloaded plug-ins. Ensure that the location to which you download the plug-ins is meant only for these missing plug-ins.

```
<software_kit>/runInstaller -plugininstall  
-pluginLocation <absolute_path_to_plugin_sw>  
-mwHome <absolute_path_to_middleware_home>  
[-invPtrLoc <absolute_path_to_oraInst.loc>]
```

The missing plug-ins displayed in the error message have the following format. Ensure that you download and install the same plug-in version and the same or higher plug-in update.

PluginID:PluginVersion:PluginUpdate

To download the missing plug-ins, follow these steps:

1. Navigate to the following location where you installed the software binaries, and check if the plug-in opar files you are looking for are available. If they are available, copy them to an accessible location.

```
$<OMS_HOME>/sysman/install/undeployed_plugins
```

2. If the opar files are not available in the OMS home, then download them from the following URL:

<http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html>

Proceed to the next step only after you have installed these missing plug-ins.

6. Provide WebLogic Server configuration details:

- If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0), then on the WebLogic Server Configuration Details screen, enter the credentials for the WebLogic Server user account and the Node Manager user account, and validate the path to the OMS instance base location.

Note: Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.

By default, the WebLogic Domain name is `GCDomain`, and the Node Manager name is `nodemanager`. These are non-editable fields. The installer uses this information for creating Oracle WebLogic Domain and other associated components such as the admin server, the managed server, and the node manager. A Node Manager enables you to start, shut down, or restart an Oracle WebLogic Server instance remotely, and is recommended for applications with high availability requirements.

- If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0), then on the Extend WebLogic Server Domain screen, validate the AdminServer host name and its port, and the WebLogic user name. Enter the WebLogic user account password for extending the existing Oracle WebLogic Server Domain to the upgraded release.

- If you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or from 11g Release 1 (11.1.0.1), then enter the host name and port of the AdminServer configured for the first OMS, and then, enter the credentials for the existing WebLogic Server user account.
7. Click **Next**.
 8. On the Tablespace Location screen, validate the location where the data file (mgmt_ad4j.dbf) for JVM Diagnostics data tablespace can be stored. You can choose to edit it if you want. In that case, ensure that the path leads up to the file name. Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).

Note: This screen appears only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0).

9. Click **Next**.
10. On the Port Configuration Details screen, customize the ports to be used for various components.
 - If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0), then you will NOT see the Port Configuration Details screen because the ports used by the old OMS and the old Management Agent will be reused by the upgraded OMS and the Management Agent. Hence, go to Step (12).
 - If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0), then on the Port Configuration Details screen, customize the ports to be used for various components.

Note: If all the ports on this screen appear as -1, then it indicates that the installer is unable to bind the ports on the host. To resolve this issue, exit the installer, verify the host name and the IP configuration of this host (ensure that the IP address of the host is not being used by another host), restart the installer, and try again.

You can enter a free custom port that is either within or outside the port range recommended by Oracle.

To verify if a port is free, run the following command:

On Unix:

```
netstat -anp | grep <port no>
```

On Microsoft Windows:

```
netstat -an|findstr <port_no>
```

However, the custom port must be greater than 1024 and lesser than 65535. Alternatively, if you already have the ports predefined in a `staticports.ini` file and if you want to use those ports, then click **Import staticports.ini File** and select the file.

Note: If the `staticports.ini` file is passed during installation, then by default, the ports defined in the `staticports.ini` file are displayed. Otherwise, the first available port from the recommended range is displayed.

11. Click **Next**.
12. On the Review screen, review the details you provided for the selected installation type.
 - If you want to change the details, click **Back** repeatedly until you reach the screen where you want to make the changes.
 - After you verify the details, if you are satisfied, click **Configure** to begin the installation process.
13. On the Install Progress screen, view the overall progress (in percentage) of the installation.

Note: If a Configuration Assistant fails, the installer stops and none of the subsequent Configuration Assistants are run until the issue related to the failed Configuration Assistant is resolved. In this case, diagnose the issue, resolve it, and then, click **Retry** on the Install Progress screen to rerun the Configuration Assistants starting from the Configuration Assistant that failed.

However, if you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home to rerun the Configuration Assistant in silent mode:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_
HOME=<absolute_path_to_oms_home> MODE=perform
ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_
0.xml}
```

14. On the Finish screen, you should see information pertaining to the installation of Enterprise Manager. Review the information and click **Close** to exit the installation wizard.

18.1.3.1 Using Advanced Script Options

The following are some additional, advanced options you can pass while invoking the `configureGC.sh` script:

- By default, `GCDomain` is the default name used for creating the WebLogic Domain. To override this and use a custom WebLogic Domain name, invoke the script with the `WLS_DOMAIN_NAME` option, and enter a unique custom name.

For example, if you want to use the custom name `EMDomain`, then run the following command:

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh WLS_
DOMAIN_NAME=EMDomain
```

- After the configuration ends successfully, the OMS and the Management Agent start automatically. If you do not want them to start automatically, then invoke the

script with `START_OMS` and `b_startAgent` options, and set them to `TRUE` or `FALSE` depending on what you want to control.

For example, if you do not want the Management Agent to start automatically, then run the following command:

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh START_OMS=TRUE b_startAgent=FALSE
```

To understand the limitations involved with this advanced option, see [Section 16.1.2](#).

18.2 Upgrading in Software-Only Mode with 2-System Upgrade Approach

This section describes how you can upgrade your OMS and Management Repository in software-only mode with 2-System upgrade approach. In particular, this section covers the following:

- [Installing Software Binaries](#)
- [Running allroot.sh Script](#)
- [Configuring and Upgrading](#)

18.2.1 Installing Software Binaries

To install the software binaries, follow the steps outlined in [Section 18.1.1](#).

Note: If the **Enterprise Manager Upload Http Port** and **Enterprise Manager Central Console Http Port** are unlocked in your existing Enterprise Manager system, then while invoking the installer, pass the arguments `ALLOW_ONLY_SECURE_ACCESS_TO_CONSOLE` and `LOCK_ORACLE_MANAGEMENT_SERVICE`.

For example,

```
<Software_Location>/runInstaller -invPtrLoc
/home/john/software/oracle/oraInst.loc ALLOW_ONLY_SECURE_ACCESS_TO_CONSOLE=FALSE LOCK_ORACLE_MANAGEMENT_SERVICE=FALSE
```

If you skip passing these arguments now, and if you want to unlock the ports later, then after upgrading the OMS, run these commands from the upgraded OMS home:

```
$<OMS_HOME>/bin/emctl secure unlock -console
$<OMS_HOME>/bin/emctl secure unlock -upload
```

18.2.2 Running allroot.sh Script

To run the `allroot.sh` script, [Section 18.1.2](#).

18.2.3 Configuring and Upgrading

To configure and upgrade your existing Enterprise Manager system, follow these steps:

1. Invoke the installation wizard by running the following script:

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh  
[-invPtrLoc <absolute_path_to_oraInst.loc>]
```

Note:

- While installing the software binaries as described in [Section 18.2.1](#), if you had passed the argument `-invPtrLoc`, then pass the same argument here as well.
 - For information about the additional, advanced options you can pass while invoking the script, refer to [Section 18.1.3.1](#).
-
-

2. On the Install Types screen, select **Upgrade an Existing Enterprise Manager System**, and then, select **Two System Upgrade**.
3. Click **Next**.
4. On the Database Connection Details screen, enter the fully qualified name of the host where the backed up database resides, its listener port and its service name or system ID (SID), and the SYS and SYSMAN user account passwords.

Note: Oracle Real Application Cluster (Oracle RAC) nodes are referred to by their virtual IP (vip) names. The `service_name` parameter is used instead of the system identifier (SID) in `connect_data` mode, and failover is turned on. For more information, refer to *Oracle Database Net Services Administrator's Guide*.

The installer uses this information to connect to the backed up database for upgrading the SYSMAN schema. SYSMAN schema holds most of the relational data used in managing Enterprise Manager Cloud Control.

5. Click **Next**.

Note:

- If you are connecting to an Oracle RAC database, and if you have entered the virtual IP address of one of its nodes, then the installation wizard prompts you with a Connection String dialog and requests you to update the connection string with information about the other nodes that are part of the cluster. Update the connection string and click **OK**. If you want to test the connection, click **Test Connection**.
 - Oracle Real Application Cluster (Oracle RAC) nodes are referred to by their virtual IP (vip) names. The `service_name` parameter is used instead of the system identifier (SID) in `connect_data` mode, and failover is turned on. For more information, refer to *Oracle Database Net Services Administrator's Guide*.
 - If you encounter a Provisioning Archive Framework (PAF) prerequisite check error, then do the following:
 - Exit the installer, run the following SQL command on the backed up database, invoke the installer all over again, and retry the upgrade process.

```
UPDATE MGMT_PAF_STATES
SET status = 6
WHERE state_type = 0
AND status IN (0, 1);
```
 - Exit the installer, discard the backed up database, stop all the running and schedule deployment procedures in your existing Enterprise Manager system, take a fresh backup of the database now, invoke the installer all over again, and retry the upgrade process.
 - If you see a warning asking you to unlock the MGMT_VIEW user account and change the password, ignore it because the installer automatically unlocks it for you.
-

Note: If you see an error about missing plug-ins, then manually download those plug-ins (opar files) to an accessible location, and invoke the installer once again in the following way to install the software binaries of the downloaded plug-ins. Ensure that the location to which you download the plug-ins is meant only for these missing plug-ins.

```
<software_kit>/runInstaller -plugininstall  
-pluginLocation <absolute_path_to_plugin_sw>  
-mwHome <absolute_path_to_middleware_home>  
[-invPtrLoc <absolute_path_to_oraInst.loc>]
```

The missing plug-ins displayed in the error message have the following format. Ensure that you download and install the same plug-in version and the same or higher plug-in update.

PluginID:PluginVersion:PluginUpdate

To download the missing plug-ins, follow these steps:

1. Navigate to the following location where you installed the software binaries, and check if the plug-in opar files you are looking for are available. If they are available, copy them to an accessible location.

```
$<OMS_HOME>/sysman/install/undeployed_plugins
```

2. If the opar files are not available in the OMS home, then download them from the following URL:

<http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html>

Proceed to the next step only after you have installed these missing plug-ins.

6. On the WebLogic Server Configuration Details screen, enter the credentials for the WebLogic Server user account and the Node Manager user account, and validate the path to the Oracle Management Service instance base location.

Note: Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.

By default, the WebLogic Domain name is GCDomain, and the Node Manager name is nodemanager. These are non-editable fields. The installer uses this information for creating Oracle WebLogic Domain and other associated components such as the admin server, the managed server, and the node manager. A Node Manager enables you to start, shut down, or restart an Oracle WebLogic Server instance remotely, and is recommended for applications with high availability requirements.

7. Click **Next**.
8. On the Old Repository Details screen, validate the connect string and enter the SYSMAN password of the old Management Repository.

The details are used to connect to the old Management Repository, check for accrued data, and seamlessly transfer it to the upgraded Management Repository.

Accrued data refers to the data that was uploaded to the old Management Repository from the time it was backed up till the time it was upgraded.

Note: Typically, the connect string is prepopulated. However, if it is not prepopulated, then enter it in the following format:

- With SID

```
(DESCRIPTION= (ADDRESS_
LIST= (ADDRESS= (PROTOCOL=TCP) (HOST=<host_
name>) (PORT=<port>))) (CONNECT_DATA= (SID=<sid>)))
```

- With Service Name

```
(DESCRIPTION= (ADDRESS_
LIST= (ADDRESS= (PROTOCOL=TCP) (HOST=<host_
name>) (PORT=<port>))) (CONNECT_DATA= (SERVICE_
NAME=<service_name>)))
```

9. Click Next.

- 10.** On the Tablespace Location screen, validate the location where the data file (mgmt_ad4j.dbf) for JVM Diagnostics data tablespace can be stored. You can choose to edit it if you want. In that case, ensure that the path leads up to the file name. Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).

Note: This screen appears only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0).

11. Click Next.

- 12.** On the Port Configuration Details screen, customize the ports to be used for various components.

- Ensure that the ports you enter for **Enterprise Manager Upload Http Port** and **Enterprise Manager Upload Http SSL Port** match with the unsecure and secure ports you entered in the *Enterprise Manager 12c Upgrade Console*.
- For other components, you can enter a free custom port that is either within or outside the port range recommended by Oracle. However, the custom port must be greater than 1024 and lesser than 65535.

To verify if a port is free, run the following command:

On Unix:

```
netstat -anp | grep <port no>
```

On Microsoft Windows:

```
netstat -an|findstr <port_no>
```

- Alternatively, if you already have the ports predefined in a `staticports.ini` file and if you want to use those ports, then click **Import staticports.ini File** and select the file.

Note: If the `staticports.ini` file is passed during installation, then by default, the ports defined in the `staticports.ini` file are displayed. Otherwise, the first available port from the recommended range is displayed. If you do pass this file, then ensure that the ports you enter for **Enterprise Manager Upload Http Port** and **Enterprise Manager Upload Http SSL Port** match with the unsecure and secure ports you entered in the *Enterprise Manager 12c Upgrade Console*.

13. Click **Next**.
14. On the Review screen, review the details you provided for the selected installation type.
 - If you want to change the details, click **Back** repeatedly until you reach the screen where you want to make the changes.
 - After you verify the details, if you are satisfied, click **Configure** to begin the installation process.
15. On the Install Progress screen, view the overall progress (in percentage) of the installation.

Note: If a Configuration Assistant fails, the installer stops and none of the subsequent Configuration Assistants are run until the issue related to the failed Configuration Assistant is resolved. In this case, diagnose the issue, resolve it, and then, click **Retry** on the Install Progress screen to rerun the Configuration Assistants starting from the Configuration Assistant that failed.

However, if you accidentally exit the installer before clicking **Retry**, then do NOT restart the installer to reach the same screen; instead, invoke the `runConfig.sh` script from the OMS home to rerun the Configuration Assistant in silent mode:

```
$<OMS_HOME>/oui/bin/runConfig.sh ORACLE_  
HOME=<absolute_path_to_oms_home> MODE=perform  
ACTION=configure COMPONENT_XML={encap_oms.1_0_0_0_  
0.xml}
```

16. On the Finish screen, you should see information pertaining to the installation of Enterprise Manager. Review the information and click **Close** to exit the installation wizard.

Installing Software Now and Upgrading Later in Silent Mode

This chapter explains how you can install only the software binaries of Enterprise Manager Cloud Control in silent mode at one point, and upgrade them at a later point.

Upgrading using the *software-only* mode in silent mode is only an alternative to upgrading in graphical mode as described in [Chapter 18](#). Therefore, the two modes work the same way. The only difference is the methodology in which you implement this installation type. While the graphical mode requires you to invoke the installer and use the interview screens to capture the installation details, the silent mode requires you to invoke the installer passing a response file that already has all the installation details captured.

This chapter covers the following:

- [Upgrading in Software-Only Mode with 1-System Upgrade Approach](#)
- [Upgrading in Software-Only Mode with 2-System Upgrade Approach](#)

Note: You can find the OMS and Management Agent entries in the `/etc/oragchomelist` file for all UNIX platforms except HPUNIX, HPia64, Solaris Sparc. On HPUNIX, HPia64, Solaris Sparc platforms, the entries are present in `/var/opt/oracle/oragchomelist`.

19.1 Upgrading in Software-Only Mode with 1-System Upgrade Approach

This section describes how you can upgrade in software-only mode with 1-System upgrade approach. In particular, this section covers the following:

- [Installing Software Binaries](#)
- [After You Install](#)
- [Configuring and Upgrading](#)

19.1.1 Installing Software Binaries

To install the software binaries of Enterprise Manager Cloud Control, follow these steps:

1. Copy the following response file to an accessible location on your local host:

```
<Software_Location>/response/software_only.rsp
```

In this command, `<Software_Location>` refers to the location where you have downloaded software kit.

2. Edit the response file and enter appropriate values for the variables described in [Table 19–1](#).
3. Invoke the installer:

```
./runInstaller -silent -responseFile <absolute_
path>/software_only.rsp [-invPtrLoc <absolute_path_to_
oraInst.loc>]
```

Note:

- To invoke the installation wizard on UNIX platforms, run `runInstaller`. To invoke on Microsoft Windows platforms, run `setup.exe`.
 - For information about the additional, advanced options you can pass while invoking the installer, refer to [Section 17.1.1](#).
 - The central inventory location you enter must NOT be on a shared file system.
-
-

4. Deinstall the Management Agent. For instructions, refer to the chapter on deinstalling a Management Agent in the *Oracle Enterprise Manager Cloud Control Advanced Installation and Configuration Guide*.

Note: The Management Agent installed with the OMS is not required because you already have the Management Agent predeployed by the *Enterprise Manager 12c Upgrade Console*.

19.1.1.1 Editing Response File for Installing Software Binaries

[Table 19–1](#) describes what variables you must edit and how you must edit them in the `software_only.rsp` response file for installing the software binaries of Enterprise Manager Cloud Control.

Table 19–1 *Editing Response File for Installing Software Binaries*

Parameter	Description
UNIX_GROUP_NAME	Enter the name of the UNIX group you belong to. For example, "dba"
INVENTORY_LOCATION	Enter the absolute path to the Central Inventory. For example, /scratch/oracle/oraInventory
SECURITY_UPDATES_VIA_MYORACLESUPPORT	<ul style="list-style-type: none"> ■ Enter TRUE if you want to download and install security updates. Then, enter the credentials for the following variables: <code>MYORACLESUPPORT_USERNAME</code> <code>MYORACLESUPPORT_PASSWORD</code> ■ Enter FALSE if you do not want to download and install security updates:

Table 19–1 (Cont.) Editing Response File for Installing Software Binaries

Parameter	Description
DECLINE_SECURITY_UPDATES	<ul style="list-style-type: none"> ■ Enter TRUE if you want to decline the security updates. In this case, you should have entered <code>False</code> for <code>SECURITY_UPDATES_VIA_MYORACLESUPPORT</code>. ■ Enter FALSE if you do not want to decline the security updates. In this case, you should have entered TRUE for <code>SECURITY_UPDATES_VIA_MYORACLESUPPORT</code>.
INSTALL_UPDATES_SELECTION	<p>By default, this variable is set to "skip" indicating that the software updates will not be installed during installation.</p> <ul style="list-style-type: none"> ■ If you want to install the software updates from My Oracle Support, then set this variable to "download". Then, enter the credentials for the following parameters: <code>MYORACLESUPPORT_USERNAME_FOR_SOFTWAREUPDATES</code> <code>MYORACLESUPPORT_PASSWORD_FOR_SOFTWAREUPDATES</code> ■ If you want to install the software updates from a staged location, then set this variable to "staged". Then, for the <code>STAGE_LOCATION</code> parameter, enter the absolute path, which leads to the <code>Updates</code> directory, where the software updates are available.
ORACLE_MIDDLEWARE_HOME_LOCATION	<p>Enter the location where you want the installer to install Oracle WebLogic Server 11g Release 1 (10.3.5) and Java Development Kit 1.6 v24.</p> <p>For example, <code>u01/app/Oracle/Middleware</code>.</p> <p>Ensure that the middleware location has <i>write</i> permission to create the Oracle homes for OMS and Management Agent.</p> <p>If you have already installed them manually, then enter the location where you have installed them.</p> <p>Note: Ensure that the middleware home you enter here is used only for Enterprise Manager Cloud Control. Ensure that no other Oracle Fusion Middleware products or components are installed in the same middleware home.</p>

Table 19–1 (Cont.) Editing Response File for Installing Software Binaries

Parameter	Description
PLUGIN_SELECTION	<p>By default, mandatory plug-ins such as Oracle Database Management Plug-In, Oracle Fusion Middleware Management Plug-In, Oracle My Oracle Support Management Plug-In, and Oracle Exadata Management Plug-In get automatically installed with the Enterprise Manager system.</p> <p>However, if you want to install any of the other optional plug-ins that are available in the software kit (DVD or downloaded software), then enter the names of those plug-ins for this variable.</p> <p>For example,</p> <pre>PLUGIN_SELECTION={"oracle.sysman.empa", "oracle.sysman.vt" }</pre> <p>If you want to install any plug-in that is not available in the software kit, then do the following:</p> <ol style="list-style-type: none"> 1. Manually download the plug-ins from the following URL, and store them in an accessible location. http://www.oracle.com/technetwork/oem/g rid-control/downloads/oem-upgrade-conso le-502238.html 2. Update this variable (PLUGIN_SELECTION) to the names of those plug-ins you downloaded. 3. Invoke the installer with the following option, and pass the location where you downloaded the plug-ins: <pre>./runInstaller -pluginLocation <absolute_path_to_plugin_software_location></pre>

19.1.2 After You Install

(For UNIX Only) After you install the software binaries, log in as a *root* user in a new terminal and run the `allroot.sh` script from the OMS home:

```
$<OMS_HOME>/allroot.sh
```

19.1.3 Configuring and Upgrading

To configure the software binaries of Enterprise Manager Cloud Control, follow these steps:

1. Copy the following response file to an accessible location on the host where you copied the software binaries of Enterprise Manager Cloud Control:

```
<Software_Location>/response/upgrade.rsp
```

In this command, `<Software_Location>` refers to the location where you have downloaded software kit.

2. Edit the response file and enter appropriate values for the variables described in [Table 19–2](#).
3. Configure the software binaries by invoking the `ConfigureGC.sh` script passing the response you edited in the previous step:

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh -silent
-responseFile <absolute_path>/upgrade.rsp [-invPtrLoc
<absolute_path_to_oraInst.loc>]
```

Note:

- While installing the software binaries as described in [Section 19.1.1](#), if you had passed the argument `-invPtrLoc`, then pass the same argument here as well.
- For information about the additional, advanced options you can pass while invoking the script, refer to [Section 18.1.3.1](#).
- If you see an error about missing plug-ins, then manually download those plug-ins (opar files) to an accessible location, and invoke the installer once again in the following way to install the software binaries of the downloaded plug-ins. Ensure that the location to which you download the plug-ins is meant only for these missing plug-ins.

```
<software_kit>/runInstaller -plugininstall
-pluginLocation <absolute_path_to_plugin_sw> -mwHome
<absolute_path_to_middleware_home> [-invPtrLoc
<absolute_path_to_oraInst.loc>]
```

The missing plug-ins displayed in the error message have the following format. Ensure that you download and install the same plug-in version and the same or higher plug-in update.

```
PluginID:PluginVersion:PluginUpdate
```

To download the missing plug-ins (opar files), follow these steps:

1. Navigate to the following location where you installed the software binaries, and check if the opar files you are looking for are available. If they are available, copy them to an accessible location.

```
$<OMS_
HOME>/sysman/install/undeployed_
plugins
```

2. If the opar files are not available in the OMS home, then download them from the following URL:

```
http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html
```

Proceed to the next step only after you have installed these missing plug-ins.

19.1.3.1 Editing Response File for Configuring Software Binaries

[Table 19–2](#) describes what variable you must update and how you must update them in the `upgrade.rsp` response file for configuring the software binaries of Enterprise Manager Cloud Control.

Table 19–2 Editing Response File for Configuring Software Binaries

Parameter	Description
ORACLE_INSTANCE_HOME_LOCATION	By default, <code>gc_inst</code> is considered as the OMS Instance Base directory for storing all OMS-related configuration files, and the by default, it is created in the middleware home. If you want to accept the default location and the directory name, then skip this variable. However, if you want to have a custom location and a custom directory name, then enter the absolute path to the custom location leading up to the custom directory name.
OLD_BASE_DIR	Enter the base directory of the OMS you want to upgrade.
ONE_SYSTEM	By default, this variable is set to <code>FALSE</code> indicating that it is 2-System upgrade. Change it to <code>TRUE</code> .
WLS_ADMIN_SERVER_USERNAME	<p><i>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</i></p> <p>By default, <code>weblogic</code> is the name assigned to the default user account that is created for the Oracle WebLogic Domain. If you want to accept the default name, then blank. However, if you want to have a custom name, then enter the name of your choice.</p> <p>Important: If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1) or if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1), then comment out this variable.</p>
WLS_ADMIN_SERVER_PASSWORD	<p><i>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</i></p> <p>Enter a password for the WebLogic user account.</p> <p>Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.</p> <p>Important: If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1) or if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1), then comment out this variable.</p>
WLS_ADMIN_SERVER_CONFIRM_PASSWORD	<p><i>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</i></p> <p>Confirm the password for the WebLogic user account.</p> <p>Important: If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1) or if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1), then comment out this variable.</p>

Table 19–2 (Cont.) Editing Response File for Configuring Software Binaries

Parameter	Description
NODE_MANAGER_PASSWORD	<p><i>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</i></p> <p>By default, nodemanager is the name assigned to the default user account that is created for the node manager. Enter a password for this node manager user account.</p> <p>Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.</p> <p>Important: If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1) or if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1), then comment out this variable.</p>
NODE_MANAGER_CONFIRM_PASSWORD	<p><i>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</i></p> <p>Confirm the password for the node manager user account.</p> <p>Important: If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1) or if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1), then comment out this variable.</p>
WLS_ADMIN_SERVER_PASSWORD	<p><i>(Applicable only if you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1))</i></p> <p>Enter the password for the WebLogic user account you had created for Enterprise Manager 11g Grid Control Release 1 (11.1.0.1).</p> <p>Important: If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1), then comment out this variable.</p>
ADMIN_SERVER_HOSTNAME	<p><i>(Applicable only if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1))</i></p> <p>Enter the host name of the AdminServer that is configured for the first OMS.</p> <p>Important: If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), then comment out this variable.</p>
ADMIN_SERVER_PORT	<p><i>(Applicable only if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1))</i></p> <p>Enter the port of the AdminServer that is configured for the first OMS.</p> <p>Important: If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), then comment out this variable.</p>

Table 19–2 (Cont.) Editing Response File for Configuring Software Binaries

Parameter	Description
WLS_ADMIN_SERVER_USERNAME	<p>(Applicable only if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1))</p> <p>By default, <code>weblogic</code> is the name assigned to the default user account that is created for the Oracle WebLogic Domain. If you want to accept the default name, then blank. However, if you want to have a custom name, then enter the name of your choice.</p> <p>Important: If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), then comment out this variable.</p>
WLS_ADMIN_SERVER_PASSWORD	<p>(Applicable only if you are upgrading an additional OMS from 10g Release 5 (10.2.0.5) or 11g Release 1 (11.1.0.1))</p> <p>Enter a password for the WebLogic user account.</p> <p>Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.</p> <p>Important: If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5) or from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), then comment out this variable.</p>
JVM_DIAGNOSTICS_TABLESPACE_LOCATION	<p>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</p> <p>Enter the absolute path to a location where the data file (<code>mgmt_ad4j.dbf</code>) for JVM Diagnostics data tablespace can be stored. Ensure that the specified path leads up to the file name.</p> <p>For example, <code>/home/john/oradata/mgmt_ad4j.dbf</code></p> <p>Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).</p>
SYS_PASSWORD	Enter the SYS user account's password.
SYSMAN_PASSWORD	Enter the SYSMAN user account's password.

Table 19–2 (Cont.) Editing Response File for Configuring Software Binaries

Parameter	Description
STATIC_PORTS_FILE	<ul style="list-style-type: none"> ■ If you are upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0), then skip this parameter because the same ports are carried over to Enterprise Manager Cloud Control. ■ If you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0), then enter the absolute path to the <code>staticports.ini</code> file that contains ONLY the following ports: Admin Server Http SSL Port Managed Server Http Port Managed Server Http SSL Port Node Manager Http SSL Port You must skip the other ports in the <code>staticports.ini</code> file because the ports used in the earlier release will be carried over to Enterprise Manager Cloud Control. The <code>staticports.ini</code> file is available in the following location of the software kit (DVD, downloaded software): <code><software_kit>/response/staticports.ini</code>

19.2 Upgrading in Software-Only Mode with 2-System Upgrade Approach

This section describes how you can upgrade in software-only mode with 2-System upgrade approach. In particular, this section covers the following:

- [Installing Software Binaries](#)
- [Running `allroot.sh` Script](#)
- [Configuring and Upgrading](#)

19.2.1 Installing Software Binaries

To install the software binaries of Enterprise Manager Cloud Control, follow the steps outlined in [Section 19.1.1](#).

Note: If the **Enterprise Manager Upload Http Port** and **Enterprise Manager Central Console Http Port** are unlocked in your existing Enterprise Manager system, then while invoking the installer, pass the arguments `ALLOW_ONLY_SECURE_ACCESS_TO_CONSOLE` and `LOCK_ORACLE_MANAGEMENT_SERVICE`.

For example,

```
<Software_Location>/runInstaller -invPtrLoc
/home/john/software/oracle/oraInst.loc ALLOW_ONLY_
SECURE_ACCESS_TO_CONSOLE=FALSE LOCK_ORACLE_
MANAGEMENT_SERVICE=FALSE
```

If you skip passing these arguments now, and if you want to unlock the ports later, then after upgrading the OMS, run these commands from the upgraded OMS home:

```
$<OMS_HOME>/bin/emctl secure unlock -console
$<OMS_HOME>/bin/emctl secure unlock -upload
```

19.2.2 Running allroot.sh Script

To run the `allroot.sh` script, [Section 19.1.2](#).

19.2.3 Configuring and Upgrading

To configure the software binaries of Enterprise Manager Cloud Control, follow these steps:

1. Copy the following response file to an accessible location on your local host:

```
<Software_Location>/response/upgrade.rsp
```

In this command, `<Software_Location>` refers to the location where you have downloaded the software kit.

2. Edit the response file and enter appropriate values for the variables described in [Table 19-3](#).
3. Configure the software binaries by invoking the `ConfigureGC.sh` script passing the response you edited in the previous step:

```
$<MIDDLEWARE_HOME>/oms/sysman/install/ConfigureGC.sh -silent
-responseFile <absolute_path>/upgrade.rsp -staticPortsIniFile
<absolute_path_to_staticports.ini_file> [-invPtrLoc
<absolute_path_to_inventory_directory>]
```

Note:

- While installing the software binaries as described in [Section 19.2.1](#), if you had passed the argument `-invPtrLoc`, then pass the same argument here as well.
- For information about the additional, advanced options you can pass while invoking the script, refer to [Section 18.1.3.1](#).
- The `staticports.ini` file is available at the following location of the software kit (DVD, downloaded software, and so on):

```
<software_kit>/response/staticports.ini
```

- In the `staticports.ini` file, ensure that the ports you enter for **Enterprise Manager Upload Http Port** and **Enterprise Manager Upload Http SSL Port** match with the unsecure and secure ports you entered in the *Enterprise Manager 12c Upgrade Console*.
- If you see an error about missing plug-ins, then manually download those plug-ins (opar files) to an accessible location, and invoke the installer once again in the following way to copy the software binaries of the downloaded plug-ins. Ensure that the location to which you download the plug-ins is meant only for these missing plug-ins.

```
<software_kit>/runInstaller -plugininstall
-pluginLocation <absolute_path_to_plugin_sw> -mwHome
<absolute_path_to_middleware_home> [-invPtrLoc
<absolute_path_to_oraInst.loc>]
```

To download the missing plug-ins (opar files), follow these steps:

1. Navigate to the following location where you installed the software binaries, and check if the opar files you are looking for are available. If they are available, copy them to an accessible location.

```
$<OMS_
HOME>/sysman/install/undeployed_
plugins
```

2. If the opar files are not available in the OMS home, then download them from the following URL:

```
http://www.oracle.com/technetwork/oem/grid-control/downloads/oem-upgrade-console-502238.html
```

Proceed to the next step only after you have installed these missing plug-ins.

Note: If you encounter any validation error, then follow these steps:

1. Discard the backed up database.
 2. Resolve the issue in the *Enterprise Manager 12c Upgrade Console*.
 3. Take a fresh backup of the database now.
 4. Invoke the installer all over again, and retry the upgrade process.
-
-

19.2.3.1 Editing Response File for Configuring Software Binaries

Table 19–3 describes how you can edit the different variables included in the `upgrade.rsp` response file.

Table 19–3 Editing Response File for Configuring Software Binaries

Parameter	Description
ORACLE_INSTANCE_HOME_LOCATION	By default, <code>gc_inst</code> is considered as the OMS Instance Base directory for storing all OMS-related configuration files, and the by default, it is created in the middleware home. If you want to accept the default location and the directory name, then skip this variable. However, if you want to have a custom location and a custom directory name, then enter the absolute path to the custom location leading up to the custom directory name.
ONE_SYSTEM	By default, this variable is set to <code>FALSE</code> indicating that it is 2-System upgrade. Retain the default value.
OLD_DATABASE_CONNECTION_DESCRIPTION	<p>Enter the connect string in the following format to connect to the old Management Repository.</p> <ul style="list-style-type: none"> ■ With SID <code>(DESCRIPTION= (ADDRESS_LIST= (ADDRESS= (PROTOCOL=TCP) (HOST=<host_name>) (PORT=<port>))) (CONNECT_DATA= (SID=<sid>)))</code> ■ With Service Name <code>(DESCRIPTION= (ADDRESS_LIST= (ADDRESS= (PROTOCOL=TCP) (HOST=<host_name>) (PORT=<port>))) (CONNECT_DATA= (SERVICE_NAME=<service_name>)))</code> <p>The connect string is used to connect to the old Management Repository, check for accrued data, and seamlessly transfer it to the upgraded Management Repository. Accrued data refers to the data that was uploaded to the old Management Repository from the time it was backed up till the time it was upgraded.</p>
OLD_DATABASE_SYSMAN_PASSWORD	Enter the SYSMAN password of the old Management Repository.
WLS_ADMIN_SERVER_USERNAME	By default, <code>weblogic</code> is the name assigned to the default user account that is created for the Oracle WebLogic Domain. If you want to accept the default name, then blank. However, if you want to have a custom name, then enter the name of your choice.
WLS_ADMIN_SERVER_PASSWORD	Enter a password for the WebLogic user account. Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.
WLS_ADMIN_SERVER_CONFIRM_PASSWORD	Confirm the password for the WebLogic user account.
NODE_MANAGER_PASSWORD	By default, <code>nodemanager</code> is the name assigned to the default user account that is created for the node manager. Enter a password for this node manager user account. Ensure that your password contains at least 8 characters without any spaces, begins with a letter, and includes at least one numeric value.

Table 19-3 (Cont.) Editing Response File for Configuring Software Binaries

Parameter	Description
NODE_MANAGER_CONFIRM_PASSWORD	Confirm the password for the node manager user account.
WLS_ADMIN_SERVER_PASSWORD	Comment out this variable.
ADMIN_SERVER_HOSTNAME	Comment out this variable.
ADMIN_SERVER_PORT	Comment out this variable.
WLS_ADMIN_SERVER_USERNAME	Comment out this variable.
WLS_ADMIN_SERVER_PASSWORD	Comment out this variable.
JVM_DIAGNOSTICS_TABLESPACE_LOCATION	<p>(Applicable only if you are upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5))</p> <p>Enter the absolute path to a location where the data file (mgmt_ad4j.dbf) for JVM Diagnostics data tablespace can be stored. Ensure that the specified path leads up to the file name.</p> <p>For example, /home/john/oradata/mgmt_ad4j.dbf</p> <p>Enterprise Manager Cloud Control requires this data file to store monitoring data related to JVM Diagnostics and Application Dependency Performance (ADP).</p>
DATABASE_HOSTNAME	<p>Enter the fully qualified name of the host where the existing database resides.</p> <p>For example, example.com</p> <p>If you are connecting to an Oracle RAC Database, and if the nodes have virtual host names, then enter the virtual host name of one of its nodes.</p> <p>The connection to the database is established with a connect string that is formed using only this virtual host name, and the installation ends successfully.</p> <p>However, if you want to update the connect string with other nodes of the cluster, then after the installation, do the following:</p> <ol style="list-style-type: none"> 1. Open the following file: <OMS_Instance_Home>/em/EMGC_OMS#/emgc.properties 2. Enter the other nodes for the variable EM_RESPOS_CONNECTDESCRIPTOR.
LISTENER_PORT	<p>Enter the listener port to connect to the existing database.</p> <p>For example, 1532</p>
SERVICENAME_OR_SID	<p>Enter the service name or the system ID (SID) of the existing database.</p> <p>For example, orcl</p>
SYS_PASSWORD	Enter the SYS user account's password.
SYSMAN_PASSWORD	Enter the SYSMAN user account's password.

Upgrading OMS and Repository for 1-System on Different Host Approach

To upgrade your existing Oracle Management Service (OMS) and Oracle Management Repository (Management Repository) with *1-System on a Different Host* approach, follow these steps:

1. On the remote host, install only the software binaries of Enterprise Manager Cloud Control.
 - For instructions to install only the software binaries in graphical mode, see [Section 18.1.1](#).
 - For instructions to install them in silent mode, see [Section 19.1.1](#).

Note that Step(15) in [Section 18.1.1](#) (graphical mode) and Step (4) in [Section 19.1.1](#) (silent mode) instruct you to deinstall the Management Agent. However, in the case of a 1-system upgrade on a different host, DO NOT deinstall the Management Agent. You need the Management Agent installed on the OMS host during the 1-system upgrade on a different host to monitor the Enterprise Manager components.

Note: This remote host must be different from the host where your existing, earlier release of Enterprise Manager is running.

2. On the host where your existing, earlier release of Enterprise Manager is running, stop the OMS. To do so, run the following command from the OMS home:

```
$<OMS_HOME>/bin/emctl stop oms -all
```

Note: On Microsoft Windows, run the following command:

```
%OMS_HOME%\bin\emctl stop oms -all
```

3. On the remote host where you installed the software binaries of Enterprise Manager Cloud Control as described in Step (1), set the environment variable ORACLE_HOME to the OMS home, and MW_HOME to the middleware home.
 - In bash terminal, run the following command:

```
export ORACLE_HOME=<absolute_path_to_oms_home>
export MW_HOME=<absolute_path_to_middleware_home>
```
 - In other terminals, run the following command:

```
setenv ORACLE_HOME <absolute_path_to_oms_home>
setenv MW_HOME <absolute_path_to_middleware_home>
```

Note: On Microsoft Windows, run the following commands:

```
set ORACLE_HOME=<absolute_path_to_middleware_home>
set MW_HOME=<absolute_path_to_middleware_home>
```

4. Run the Management Repository-related prerequisite checks to verify if the Oracle Management Repository (Management Repository) its ready for upgrade:

- a. Create a directory for storing prerequisite results:

```
mkdir <prereq_result_location>
```

Example for UNIX platforms:

```
mkdir $ORACLE_HOME/prerequisiteResults
```

Note: Example for Microsoft Windows:

```
mkdir %ORACLE_HOME%\prerequisiteResults
```

- b. Run the prerequisite checks:

```
$ORACLE_HOME/install/requisites/bin/emprereqkit
-executionType upgrade -prerequisiteXMLLoc $ORACLE_
HOME/install/requisites/list -prereqResultLoc <prereq_
result_location> -dbHost <REPOSITORY_HOST> -dbPort <PORT>
-dbSid <REPOSITORY_SID> -dbUser SYS -dbPassword <db_
password> -reposUser sysman -reposPassword <repo_user_
password> -dbRole sysdba -runPrerequisites
```

Note: On Microsoft Windows, run the following command:

```
%ORACLE_HOME%\install\requisites\bin\emprereqkit.bat
-executionType upgrade -prerequisiteXMLLoc %ORACLE_
HOME%\install\requisites\list -prereqResultLoc
<prereq_result_location> -dbHost <REPOSITORY_HOST>
-dbPort <PORT> -dbSid <REPOSITORY_SID> -dbUser SYS
-dbPassword <db_password> -reposUser sysman
-reposPassword <repo_user_password> -dbRole sysdba
-runPrerequisites
```

For example,

```
$ORACLE_HOME/install/requisites/bin/emprereqkit
-executionType upgrade -prerequisiteXMLLoc $ORACLE_
HOME/install/requisites/list -prereqResultLoc $ORACLE_
HOME/prerequisiteResults -dbHost example.com -dbPort 1521
-dbSid dbview -dbUser SYS -dbPassword dbpass -reposUser
sysman -reposPassword repopass -dbRole sysdba
-runPrerequisites
```

Note: Example for Microsoft Windows:

```
%ORACLE_HOME%\install\requisites\bin\emprereqkit.bat
-executionType upgrade -prerequisiteXMLLoc %ORACLE_
HOME%\install\requisites\list -prereqResultLoc
%ORACLE_HOME%\prerequisiteResults -dbHost
example.com -dbPort 1521 -dbSid dbview -dbUser SYS
-dbPassword dbpass -reposUser sysman -reposPassword
repopass -dbRole sysdba -runPrerequisites
```

Note: The output of this step confirms the prerequisite checks that passed and failed. You will see the status *Pass* or *Fail*.

5. If the Management Repository-related prerequisite checks fail, run the post-corrective actions to automatically correct the issues:

```
$ORACLE_HOME/install/requisites/bin/emprereqkit
-executionType upgrade -prerequisiteXMLLoc $ORACLE_
HOME/install/requisites/list -prereqResultLoc <prereq_result_
location> -dbHost <REPOSITORY_HOST> -dbPort <PORT> -dbSid
<REPOSITORY_SID> -dbUser SYS -dbPassword <db_password>
-reposUser sysman -reposPassword <repo_user_password> -dbRole
sysdba -useHistory -runCorrectiveActions
```

Note: On Microsoft Windows, run the following command:

```
%ORACLE_HOME%\install\requisites\bin\emprereqkit.bat
-executionType upgrade -prerequisiteXMLLoc %ORACLE_
HOME%\install\requisites\list -prereqResultLoc
<prereq_result_location> -dbHost <REPOSITORY_HOST>
-dbPort <PORT> -dbSid <REPOSITORY_SID> -dbUser SYS
-dbPassword <db_password> -reposUser sysman
-reposPassword <repo_user_password> -dbRole sysdba
-useHistory -runCorrectiveActions
```

For example,

```
$ORACLE_HOME/install/requisites/bin/emprereqkit
-executionType upgrade -prerequisiteXMLLoc $ORACLE_
HOME/install/requisites/list -prereqResultLoc $ORACLE_
HOME/prerequisiteResults -dbHost example.com -dbPort 1521
-dbSid dbview -dbUser SYS -dbPassword dbpass -reposUser
sysman -reposPassword repopass -dbRole sysdba -useHistory
-runCorrectiveActions
```

Note: Example for Microsoft Windows:

```
%ORACLE_HOME%\install\requisites\bin\emprereqkit.bat
-executionType upgrade -prerequisiteXMLLoc %ORACLE_
HOME%\install\requisites\list -prereqResultLoc
%ORACLE_HOME%\prerequisiteResults -dbHost
example.com -dbPort 1521 -dbSid dbview -dbUser SYS
-dbPassword dbpass -reposUser sysman -reposPassword
repopass -dbRole sysdba -useHistory
-runCorrectiveActions
```

Note: The output of this step confirms whether or not corrective actions were taken by the script. If corrective actions were taken by the script, then you will see the status *Pass*. Otherwise, you will see the status *NA*.

If the status of the prerequisite check was *Fail* in the output of Step (4), and if it changed to *NA* in the output of Step (5), do the following:

1. Access the following file:

On UNIX platforms:

```
$ORACLE_
HOME/prerequisiteResults/log/LATEST/emprereqkit.o
ut
```

On Microsoft Windows platforms:

```
%ORACLE_
HOME%\prerequisiteResults\log\LATEST\emprereqkit.
out
```

2. Review the passed and failed tests and their corresponding corrective actions.
 3. For the failed tests, manually take corrective actions.
-
-

6. Run the plug-in configuration assistant in prerequisite mode:

```
$ORACLE_HOME/bin/pluginca -oracleHome $ORACLE_HOME
-middlewareHome $MW_HOME -action prereqCheck -plugins <list_
of_plugins> -oldOracleHome <old_oms_home> -installMode
gcUpgrade -client gcinstaller -customParams
"connectString=(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=<REPOSITORY_
HOST>) (PORT=<PORT>))) (CONNECT_DATA=(SID=<REPOSITORY_
SID>)),username=sysman"
```

Note: The plug-ins to be mentioned for the `<pluginslist>` argument can be found in the following file:

```
$ORACLE_HOME/sysman/install/plugins_installed.txt
```

Note: On Microsoft Windows, run the following command:

```
%ORACLE_HOME%\bin\pluginca -oracleHome %ORACLE_HOME%
-middlewareHome %MW_HOME% -action prereqCheck
-plugins <list_of_plugins> -oldOracleHome <old_oms_
home> -installMode gcUpgrade -client gcinstaller
-customParams "connectString=(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=<REPOSITORY_
HOST>) (PORT=<PORT>))) (CONNECT_DATA=(SID=<REPOSITORY_
SID>)),username=sysman"
```

For example,

```
$ORACLE_HOME/bin/pluginca -oracleHome $ORACLE_HOME
-middlewareHome $MW_HOME -action prereqCheck -plugins
"oracle.sysman.db=12.1.0.1.0,oracle.sysman.xa=12.1.0.1.0,oracle.
sysman.emas=12.1.0.1.0,oracle.sysman.mos=12.1.0.1.0,oracle
.em.sat=12.1.0.1.0,oracle.em.sidb=12.1.0.1.0,oracle.em.smdn=1
2.1.0.1.0,oracle.em.smad=12.1.0.1.0,oracle.em.smss=12.1.0.1.0
,oracle.sysman.emct=12.1.0.1.0,oracle.sysman.ssa=12.1.0.1.0,o
racle.sysman.emfa=12.1.0.1.0,oracle.sysman.empa=12.1.0.1.0,or
acle.sysman.vt=12.1.0.1.0,oracle.em.ssad=12.1.0.1.0"
-oldOracleHome <old_oms_home> -installMode gcUpgrade -client
gcinstaller -customParams
"connectString=(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=example.com) (PORT=1521))) (C
ONNECT_DATA=(SID=dbview)),username=sysman"
```

Note: Ensure that the old OMS home is accessible from the remote host where you are running this command.

Note: Example for Microsoft Windows:

```
%ORACLE_HOME%\bin\pluginca -oracleHome %ORACLE_HOME%
-middlewareHome %MW_HOME% -action prereqCheck
-plugins
"oracle.sysman.db=12.1.0.1.0,oracle.sysman.xa=12.1.0
.1.0,oracle.sysman.emas=12.1.0.1.0,oracle.sysman.mos
=12.1.0.1.0,oracle.em.sat=12.1.0.1.0,oracle.em.sidb=
12.1.0.1.0,oracle.em.smdn=12.1.0.1.0,oracle.em.smad=
12.1.0.1.0,oracle.em.smss=12.1.0.1.0,oracle.sysman.e
mct=12.1.0.1.0,oracle.sysman.ssa=12.1.0.1.0,oracle.s
ysman.emfa=12.1.0.1.0,oracle.sysman.empa=12.1.0.1.0,
oracle.sysman.vt=12.1.0.1.0,oracle.em.ssad=12.1.0.1.
0" -oldOracleHome \\oldem\c$\EM\oms10g -installMode
gcUpgrade -client gcinstaller -customParams
"connectString=(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=example.com) (PORT=
1521))) (CONNECT_DATA=(SID=dbview)),username=sysman"
```

7. Run Management Repository-related preupgrade checks:

```
$ORACLE_HOME/sysman/admin/emdrep/bin/RepManager -doPurging
yes <REPOSITORY_HOST> <PORT> <REPOSITORY_SID> -action
preupgrade -dbUser SYS -reposName sysman -mwHome $MW_HOME
-mwOraHome $ORACLE_HOME -oracleHome $ORACLE_HOME
```

Note: On Microsoft Windows, run the following command:

```
%ORACLE_HOME%\sysman\admin\emdrep\bin\RepManager
-doPurging yes <REPOSITORY_HOST> <PORT> <REPOSITORY_
SID> -action preupgrade -dbUser SYS -reposName
sysman -mwHome %MW_HOME% -mwOraHome %ORACLE_HOME%
-oracleHome %ORACLE_HOME%
```

For example,

```
$ORACLE_HOME/sysman/admin/emdrep/bin/RepManager -doPurging
yes example.com 1521 dbview -action preupgrade -dbUser SYS
-reposName sysman -mwHome $MW_HOME -mwOraHome $ORACLE_HOME
-oracleHome $ORACLE_HOME
```

Note: Example for Microsoft Windows:

```
%ORACLE_HOME%\sysman\admin\emdrep\bin>RepManager
-doPurging yes example.com 1521 dbview -action
preupgrade -dbUser SYS -reposName sysman -mwHome
%MW_HOME% -mwOraHome %ORACLE_HOME% -oracleHome
%ORACLE_HOME%
```

8. Upgrade the Management Repository:

```
$ORACLE_HOME/sysman/admin/emdrep/bin/RepManager -doPurging
yes -connectString "(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=<REPOSITORY_HOST>
) (PORT=<PORT>))) (CONNECT_DATA=(SID=<REPOSITORY SID>)))"
-action upgrade -dbUser SYS -reposName sysman -mwHome $MW_
HOME -mwOraHome $ORACLE_HOME -oracleHome $ORACLE_HOME
```

If the preceding command fails, then run the following:

```
$ORACLE_HOME/sysman/admin/emdrep/bin/RepManager -doPurging
yes -connectString "(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=<REPOSITORY_HOST>
) (PORT=<PORT>))) (CONNECT_DATA=(SID=<REPOSITORY SID>)))"
-resume retry -checkpointLocation $ORACLE_
HOME/sysman/log/schemamanager -dbUser SYS -reposName sysman
-mwHome $MW_HOME -mwOraHome $ORACLE_HOME -oracleHome $ORACLE_
HOME
```

Note: On Microsoft Windows, run the following command:

```
%ORACLE_HOME%\sysman\admin\emdrep\bin\RepManager
-doPurging yes -connectString
"(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<REPOSITORY_HOST>
)(PORT=<PORT>)))(CONNECT_DATA=(SID=<REPOSITORY
SID>)))" -action upgrade -dbUser SYS -reposName
sysman -mwHome %MW_HOME% -mwOraHome %ORACLE_HOME%
-oracleHome %ORACLE_HOME%
```

If the preceding command fails, then run the following:

```
%ORACLE_HOME%\sysman\admin\emdrep\bin\RepManager
-doPurging yes -connectString
"(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<REPOSITORY_HOST>
)(PORT=<PORT>)))(CONNECT_DATA=(SID=<REPOSITORY
SID>)))" -resume retry -checkpointLocation $ORACLE_
HOME/sysman/log/schemamanager -dbUser SYS
-reposName sysman -mwHome %MW_HOME% -mwOraHome
%ORACLE_HOME% -oracleHome %ORACLE_HOME%
```

For example,

```
$ORACLE_HOME/sysman/admin/emdrep/bin/RepManager -doPurging
yes -connectString "(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<example.com>
)(PORT=1521)))(CONNECT_DATA=(SID=dbview)))" -action upgrade
-dbUser SYS -reposName sysman -mwHome $MW_HOME -mwOraHome
$ORACLE_HOME -oracleHome $ORACLE_HOME
```

Note: Example for Microsoft Windows:

```
%ORACLE_HOME%\sysman\admin\emdrep\bin\RepManager
-doPurging yes -connectString
"(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=example.com)(PORT=
1521)))(CONNECT_DATA=(SID=dbview)))" -action upgrade
-dbUser SYS -reposName sysman -mwHome %MW_HOME%
-mwOraHome %ORACLE_HOME% -oracleHome %ORACLE_HOME%
```

9. Revert the corrective actions that were automatically taken in Step (5):

```
$ORACLE_HOME/install/requisites/bin/emprereqkit
-executionType upgrade -prerequisiteXMLLoc $ORACLE_
HOME/install/requisites/list -prereqResultLoc <prereq_result_
location> -connectString "(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<REPOSITORY_HOST>
)(PORT=<PORT>)))(CONNECT_DATA=(SID=<REPOSITORY_SID>)))"
-dbUser SYS -dbPassword <db_password> -reposUser sysman
-reposPassword <repo_user_password> -dbRole sysdba
-useHistory -runPostCorrectiveActions
```

Note: On Microsoft Windows, run the following command:

```
%ORACLE_HOME%\install\requisites\bin\emprereqkit.bat
-executionType upgrade -prerequisiteXMLLoc %ORACLE_
HOME%\install\requisites\list -prereqResultLoc
<prereq_result_location> -connectString
" (DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=<REPOSITORY_HOST>
) (PORT=<PORT>))) (CONNECT_DATA=(SID=<REPOSITORY_
SID>)))" -dbUser SYS -dbPassword <db_password>
-reposUser sysman -reposPassword <repo_user_
password> -dbRole sysdba -useHistory
-runPostCorrectiveActions
```

For example,

```
$ORACLE_HOME/install/requisites/bin/emprereqkit
-executionType upgrade -prerequisiteXMLLoc $ORACLE_
HOME/install/requisites/list -prereqResultLoc $ORACLE_
HOME/prerequisiteResults -connectString
" (DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=example.com) (PORT=1521))) (C
ONNECT_DATA=(SID=dbview)))" -dbUser SYS -dbPassword dbpass
-reposUser sysman -reposPassword repopass -dbRole sysdba
-useHistory -runPostCorrectiveActions
```

Note: Example for Microsoft Windows:

```
%ORACLE_
HOME%\install\requisites\bin\emprereqkit.bat
-executionType upgrade -prerequisiteXMLLoc %ORACLE_
HOME%\install\requisites\list -prereqResultLoc
%ORACLE_HOME%\prerequisiteResults -connectString
" (DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=example.com) (PORT=
1521))) (CONNECT_DATA=(SID=dbview)))" -dbUser SYS
-dbPassword dbpass -reposUser sysman -reposPassword
repopass -dbRole sysdba -useHistory
-runPostCorrectiveActions
```

10. Create MDS schema in the Management Repository:

```
$ORACLE_HOME/perl/bin/perl $ORACLE_
HOME/sysman/admin/emdrep/bin/mdsschemamanager.pl
-action=createRepository -connectString=<REPOSITORY_
HOST>:<PORT>:<REPOSITORY_SID> -dbUser=SYS -dbPassword=<db_
password> -mdsPassword=<new_mds_user_password> -mwHome=$MW_
HOME
```

Note: On Microsoft Windows, run the following command:

```
%ORACLE_HOME%\perl\bin\perl %ORACLE_
HOME%\sysman\admin\emdrep\bin\mdsschemamanager.pl
-action=-createRepository
-connectString=<REPOSITORY_HOST>:<PORT>:<REPOSITORY_
SID> -dbUser=SYS -dbPassword=<db_password>
-mdsPassword=<new_mds_user_password> -mwHome=%MW_
HOME%
```

For example,

```
$ORACLE_HOME/perl/bin/perl $ORACLE_
HOME/sysman/admin/emdrep/bin/mdsschemamanager.pl
-action=-createRepository
-connectString=example.com:1521:dbview -dbUser=SYS
-dbPassword=dbpass -mdsPassword=mdspass -mwHome=$MW_HOME
```

Note: Example for Microsoft Windows:

```
%ORACLE_HOME%\perl\bin\perl %ORACLE_
HOME%\sysman\admin\emdrep\bin\mdsschemamanager.pl
-action=-createRepository
-connectString=example.com:1521:dbview -dbUser=SYS
-dbPassword=dbpass -mdsPassword=mdspass -mwHome=%MW_
HOME%
```

11. Create OPS schema in the Management Repository:

```
$ORACLE_HOME/sysman/admin/emdrep/bin/SecurityRepManager
-action createRepository -connectString
"(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<REPOSITORY_
HOST>)(PORT=<PORT>)))(CONNECT_DATA=(SID=<REPOSITORY_
SID>)))"
-dbUser SYS -dbPassword <db_password> -schemaPrefix sysman
-schemaPassword <sysman_user_password> -component opss
```

Note: On Microsoft Windows, run the following command:

```
%ORACLE_
HOME%\sysman\admin\emdrep\bin\SecurityRepManager
-action createRepository -connectString
"(DESCRIPTION=(ADDRESS_
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=<REPOSITORY_
HOST>)(PORT=<PORT>)))(CONNECT_DATA=(SID=<REPOSITORY_
SID>)))" -dbUser SYS -dbPassword <db_password>
-schemaPrefix sysman -schemaPassword <sysman_user_
password> -component opss
```

For example,

```
$ORACLE_HOME/sysman/admin/emdrep/bin/SecurityRepManager
-action createRepository -connectString
"(DESCRIPTION=(ADDRESS_
```

```
LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=example.com)(PORT=1521))(CONNECT_DATA=(SID=dbview))" -dbUser SYS -dbPassword dbpass -schemaPrefix sysman -schemaPassword sysmanpass -component opss
```

Note: Example for Microsoft Windows:

```
%ORACLE_HOME%\sysman\admin\emdrep\bin\SecurityRepManager -action createRepository -connectString "(DESCRIPTION=(ADDRESS_LIST=(ADDRESS=(PROTOCOL=TCP)(HOST=example.com)(PORT=1521))(CONNECT_DATA=(SID=dbview)))" -dbUser SYS -dbPassword dbpass -schemaPrefix sysman -schemaPassword sysmanpass -component opss
```

12. Configure the OMS:

```
$ORACLE_HOME/bin/omsca NEW -lock_console -lock_upload -CONFIGURE_REPEATER true -nostart [-RESPONSE_FILE <absolute_location_to_response_file>]
```

Note: On Microsoft Windows, run the following command:

```
%ORACLE_HOME%\bin\omsca NEW -lock_console -lock_upload -CONFIGURE_REPEATER true -nostart [-RESPONSE_FILE <absolute_location_to_response_file>]
```

Note: The argument `-RESPONSE_FILE <absolute_location_to_response_file>` is optional.

The response file must contain the following variables:

```
-AS_HOST=<hostname>
-AS_USERNAME=<admin server username>
-AS_HTTPS_PORT=<admin server https port>
-MSPORT=<managed server http port>
-MS_HTTPS_PORT=<managed server https port>
-EM_INSTANCE_HOME=<MW_HOME/gc_inst by default>
-EM_NODEMGR_PORT=<node manager https port>
-WEBTIER_ORACLE_HOME=<MW_HOME/Oracle_WT>
-REP_USER=SYSMAN
-REP_CONN_STR=<connection string>
-NM_USER=<node manager username>
-EM_DOMAIN_NAME=<domain name>
-EM_INSTANCE_HOST=<hostname where the instance home will reside>
-EM_UPLOAD_PORT=<upload http port>
-EM_UPLOAD_HTTPS_PORT=<upload https port>
-EM_CONSOLE_PORT=<console http port>
-EM_CONSOLE_HTTPS_PORT=<console https port>
```

Example 20-1 Reponse File Format for UNIX

```
-AS_HOST=example.com
-AS_USERNAME=weblogic
```

```
-AS_HTTPS_PORT=7101
-MSPORT=7201
-MS_HTTPS_PORT=7301
-EM_INSTANCE_HOME=/home/john/oracle/em/middleware/gc_inst
-EM_NODEMGR_PORT=7401
-WEBTIER_ORACLE_HOME=/home/john/oracle/em/middleware/Oracle_WT
-REP_USER=SYSMAN
-REP_CONN_STR=(DESCRIPTION=(ADDRESS_
LIST\=(ADDRESS\=(PROTOCOL=TCP) (HOST=example.com) (PORT=1521))) (CONNECT_
DATA\=(SID=dbview)))
-NM_USER=nodemanager
-EM_DOMAIN_NAME=GCDomain
-EM_INSTANCE_HOST=example.com
-EM_UPLOAD_PORT=4889
-EM_UPLOAD_HTTPS_PORT=1159
-EM_CONSOLE_PORT=7788
-EM_CONSOLE_HTTPS_PORT=7799
```

Example 20–2 *Response File Format for Microsoft Windows*

```
-AS_HOST=example.com
-AS_USERNAME=weblogic
-AS_HTTPS_PORT=7101
-MSPORT=7201
-MS_HTTPS_PORT=7301
-EM_INSTANCE_HOME=C:\\Oracle\\Middleware\\gc_inst
-EM_NODEMGR_PORT=7401
-WEBTIER_ORACLE_HOME=C:\\Oracle\\Middleware\\Oracle_WT
-REP_USER=SYSMAN
-REP_CONN_STR=(DESCRIPTION=(ADDRESS_
LIST\=(ADDRESS\=(PROTOCOL=TCP) (HOST=example.com) (PORT=1521))) (CONNECT_
DATA\=(SID=dbview)))
-NM_USER=nodemanager
-EM_DOMAIN_NAME=GCDomain
-EM_INSTANCE_HOST=example.com
-EM_UPLOAD_PORT=4889
-EM_UPLOAD_HTTPS_PORT=1159
-EM_CONSOLE_PORT=7788
-EM_CONSOLE_HTTPS_PORT=7799
```

13. Configure the plug-ins:

```
$ORACLE_HOME/bin/pluginca -oracleHome $ORACLE_HOME
-middlewreHome $MW_HOME -action deploy -plugins <pluginlist>
-oldOracleHome <old_oms_home> -installMode gcupgrade
```

Note: The plug-ins to be mentioned for the <pluginlist> argument can be found in the following file:

```
$ORACLE_HOME/sysman/install/plugins_installed.txt
```

Note: On Microsoft Windows, run the following command:

```
%ORACLE_HOME%\bin\pluginca -oracleHome %ORACLE_HOME%
-middlewreHome %MW_HOME% -action deploy -plugins
"<pluginlist>" -oldOracleHome <old_oms_home>
-installMode gcupgrade
```

For example,

```
$ORACLE_HOME/bin/pluginca -oracleHome $ORACLE_HOME
-middlewareHome $MW_HOME -action deploy -plugins
"oracle.sysman.db=12.1.0.1.0,oracle.sysman.xa=12.1.0.1.0,oracle.sysman.emas=12.1.0.1.0,oracle.sysman.mos=12.1.0.1.0,oracle.em.sat=12.1.0.1.0,oracle.em.sidb=12.1.0.1.0,oracle.em.smdn=12.1.0.1.0,oracle.em.smad=12.1.0.1.0,oracle.em.smss=12.1.0.1.0,oracle.sysman.emct=12.1.0.1.0,oracle.sysman.ssa=12.1.0.1.0,oracle.sysman.emfa=12.1.0.1.0,oracle.sysman.empa=12.1.0.1.0,oracle.sysman.vt=12.1.0.1.0,oracle.em.ssad=12.1.0.1.0"
-oldOracleHome /u02/app/Oracle/Middleware/oms11g -installMode gcupgrade
```

Note: Ensure that the old OMS home is accessible from the remote host where you are running this command.

Note: Example for Microsoft Windows:

```
%ORACLE_HOME%\bin\pluginca -oracleHome %ORACLE_HOME%
-middlewareHome %MW_HOME% -action deploy -plugins
"oracle.sysman.db=12.1.0.1.0,oracle.sysman.xa=12.1.0.1.0,oracle.sysman.emas=12.1.0.1.0,oracle.sysman.mos=12.1.0.1.0,oracle.em.sat=12.1.0.1.0,oracle.em.sidb=12.1.0.1.0,oracle.em.smdn=12.1.0.1.0,oracle.em.smad=12.1.0.1.0,oracle.em.smss=12.1.0.1.0,oracle.sysman.emct=12.1.0.1.0,oracle.sysman.ssa=12.1.0.1.0,oracle.sysman.emfa=12.1.0.1.0,oracle.sysman.empa=12.1.0.1.0,oracle.sysman.vt=12.1.0.1.0,oracle.em.ssad=12.1.0.1.0" -oldOracleHome \\comp1\c$\EM\oms10g -installMode gcupgrade
```

14. Migrate the plug-in inventory from old tables to the new Plug-In Lifecycle Application (PLA) inventory table:

- a.** Log in to the upgraded Management Repository as SYSMAN user:

From the Old OMS

Navigate to the \$DB_HOME\bin directory.

For example (UNIX), /scratch/aime/DB/db/bin. For example (Microsoft Windows), C:\DB\db\bin.

Run the following, where HOST is where the Management Repository resides:

```
sqlplus sysman/<password_for_sysman_
user>@" (DESCRIPTION= (ADDRESS= (PROTOCOL=TCP) (HOST=<REPOSITO
RY_HOST>) (PORT=<PORT>)) (CONNECT_
DATA= (SERVER=DEDICATED) (SERVICE_NAME=<REPOSITORY_SID>)) )
```

For example,

```
sqlplus
sysman/mypwd@" (DESCRIPTION= (ADDRESS= (PROTOCOL=TCP) (HOST=ex
ample.com) (PORT=1521)) (CONNECT_
DATA= (SERVER=DEDICATED) (SERVICE_NAME=dbview)) )
```

From the New OMS

Navigate to the `$MW_HOME\oms\bin` directory.

Run the following:

```
sqlplus sysman/<password _for_sysman_
user>@" (DESCRIPTION= (ADDRESS= (PROTOCOL=TCP) (HOST=<REPOSITO
RY_HOST>) (PORT=<PORT>)) (CONNECT_
DATA= (SERVER=DEDICATED) (SERVICE_NAME=<REPOSITORY_SID>)) ) "
```

For example,

```
sqlplus
sysman/mypwd@" (DESCRIPTION= (ADDRESS= (PROTOCOL=TCP) (HOST=ex
ample.com) (PORT=1521)) (CONNECT_
DATA= (SERVER=DEDICATED) (SERVICE_NAME=dbview)) ) "
```

b. Run the following SQL query

```
SET SERVEROUTPUT ON SIZE 100000
DECLARE
PLUGIN_BITS_TYPE      CONSTANT NUMBER := 1;
DISCOVERY_BITS_TYPE   CONSTANT NUMBER := 2;
AGENT_DEST_TYPE       CONSTANT NUMBER := 3;
err_num NUMBER;
err_msg VARCHAR2(100);

BEGIN
    FOR rec in ( select plugin_id, plugin_version, target_guid, plugin_
home, plugin_type from PRE_UPGC_DEP_PLUGINS )
LOOP

BEGIN

IF rec.plugin_type = 'discoveryplugin' THEN
EM_PLUGIN_INVENTORY.add_to_plugin_inventory(rec.plugin_id, rec.plugin_
version, DISCOVERY_BITS_TYPE, AGENT_DEST_TYPE, rec.target_guid, rec.plugin_
home);
ELSE
EM_PLUGIN_INVENTORY.add_to_plugin_inventory(rec.plugin_id, rec.plugin_
version, PLUGIN_BITS_TYPE, AGENT_DEST_TYPE, rec.target_guid, rec.plugin_
home);
END IF;

EXCEPTION
WHEN DUP_VAL_ON_INDEX THEN
-- ALTER SESSION CLOSE DATABASE LINK PREUPGTO_NG_LINK;
DBMS_OUTPUT.PUT_LINE('Records already exists. ');
WHEN OTHERS THEN
-- ALTER SESSION CLOSE DATABASE LINK PREUPGTO_NG_LINK;
err_num := SQLCODE;
err_msg := SUBSTR(SQLERRM, 1, 100);
DBMS_OUTPUT.PUT_LINE('Found exception Error Message : ' || err_msg || '
Error Number ;' || err_num);

END;

END LOOP;
commit;
END;
```

15. Start the OMS:

```
$ORACLE_HOME/bin/emctl start oms
```

Note: On Microsoft Windows, run the following command:

```
%ORACLE_HOME%\bin\emctl start oms
```

16. While installing the software binaries in Step (1), if you had chosen to configure the security updates, then configure Oracle Configure Manager (OCM):

```
$ORACLE_HOME/perl/bin/perl $ORACLE_
HOME/sysman/install/RunOMSOCMConfig.pl $ORACLE_HOME $ORACLE_
HOME/perl/bin/perl
```

Note: On Microsoft Windows, run the following command:

```
%ORACLE_HOME%\perl\bin\perl %ORACLE_
HOME%\sysman\install\RunOMSOCMConfig.pl %ORACLE_
HOME% %ORACLE_HOME%\perl\bin\perl
```

17. Configure the Management Agent. To do so, run the following command from the Management Agent home:

```
$ORACLE_HOME/sysman/install/agentDeploy.sh AGENT_BASE_
DIR=<absolute_path_to_agentbasedir> OMS_HOST=<oms_host> EM_
UPLOAD_PORT=<secure_oms_upload_port> AGENT_REGISTRATION_
PASSWORD=<agent_reg_password> -configOnly
```

Note: On Microsoft Windows, run the following command:

```
$ORACLE_HOME\sysman\install\agentDeploy.bat AGENT_
BASE_DIR=<absolute_path_to_agentbasedir> OMS_
HOST=<oms_host> EM_UPLOAD_PORT=<secure_oms_upload_
port> AGENT_REGISTRATION_PASSWORD=<agent_reg_
password> -configOnly
```

For example,

```
/u01/app/Oracle/Middleware/agent/core/12.1.0.1.0/sysman/insta
ll/agentDeploy.sh AGENT_BASE_
DIR=/u01/app/Oracle/Middleware/agent OMS_HOST=example.com EM_
UPLOAD_PORT=1159 AGENT_REGISTRATION_PASSWORD=2bornot2b
-configOnly
```

Note: Ensure that you enter the secure (HTTPS) upload port number for the argument EM_UPLOAD_PORT.

Note: Example for Microsoft Windows:

```
C:\Oracle\Middleware\agent\core\12.1.0.1.0\sysman\install\agentDeploy.bat AGENT_BASE_  
DIR=C:\Oracle\Middleware\agent OMS_HOST=example.com  
EM_UPLOAD_PORT=1159 AGENT_REGISTRATION_  
PASSWORD=2bornot2b -configOnly
```

Upgrading Multi-OMS Environment

To upgrade an Enterprise Manager system that has multiple OMS, follow these steps:

1. Upgrade the first OMS along with the Management Agents in your system. You can use any of the upgrade approaches described in this guide — [Chapter 4](#), [Chapter 5](#), or [Chapter 6](#).
2. After upgrading the first OMS in your system, do the following:
 - If you upgraded the first OMS with 2-System upgrade approach, then for every other host where an additional OMS of the earlier release is running, install a new Oracle Management Service 12c using the *Add Management Service* deployment procedure available in the Enterprise Manager Cloud Control console.

For information about installing an additional OMS using the *Add Management Service* deployment procedure, refer to the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

- If you upgraded the first OMS with 1-System upgrade approach, then for every other host where an additional OMS of the earlier release is running, invoke the Enterprise Manager Cloud Control Installation Wizard, and on the Install Types screen, select **Upgrade an Existing Enterprise Manager System**, and then, select **One System Upgrade**. Then, select the OMS home you want to upgrade.

Part VI

Postupgrade Steps

This part describes the postinstallation tasks you must perform. In particular, this part covers the following:

- [Chapter 22, "Creating Link to Upgraded Oracle Management Repository"](#)
- [Chapter 23, "Reconfiguring Oracle Software Library"](#)
- [Chapter 24, "Checking Agent Upgrade Status"](#)
- [Chapter 25, "Performing General Postupgrade Tasks"](#)
- [Chapter 26, "Tracking the Status of Deferred Data Migration Jobs"](#)
- [Chapter 27, "Tracking the Status of Accrued Data Migration Jobs"](#)
- [Chapter 28, "Generating and Viewing Diff Reports"](#)
- [Chapter 29, "Viewing Inactive Targets in the Upgraded Enterprise Manager System"](#)
- [Chapter 30, "Signing Off Accrued Data Migration Process"](#)
- [Chapter 31, "Updating Incident Rules"](#)

Creating Link to Upgraded Oracle Management Repository

Note: Follow these instructions only if you are upgrading using the 2-System upgrade approach. Perform these steps in the Enterprise Manager Grid Control console of the earlier release.

As a prerequisite for upgrading your Enterprise Manager system using the 2-System upgrade approach, you are required to back up your existing database first, and then upgrade the Oracle Management Repository (Management Repository) that is configured in it. This is to ensure that the upgraded Management Repository coexists with the earlier release of the Management Repository.

However, after you upgrade the Management Repository in the backed up database, link it to your earlier release of the Management Repository so that the two repositories are linked with each other, and any operations on the upgraded repository can be directly done from the old repository.

To link the earlier release of the repository to the upgraded repository, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, in the Select Upgrade Type section, select **2-System**. For information about these upgrade approaches, see "Understanding Upgrade Approaches".

Enterprise Manager Grid Control refreshes the page and displays a table with a list of tasks you need to perform for the upgrade approach you selected.

4. In the OMS Upgrade Steps section, from the table, click **Create Link to Upgraded Repository**.
5. On the Create Upgraded Oracle Management Repository Link page, in the Repository Link Details section, do the following:
 - a. Enter the connect string to connect to the upgraded Management Repository that will be used by Enterprise Manager Cloud Control.

Note: You will find the connect string set as a value to the EM_REPOS_CONNECTDESCRIPTOR parameter of the emgc.properties file. This file is present in the OMS Instance Base directory (gc_inst). When you enter this value as the connect string, remove all backslashes (\) and white spaces if any.

For example, the value in the emgc.properties file might be:

```
(DESCRIPTION\=(ADDRESS_  
LIST\=(ADDRESS\=(PROTOCOL\=TCP) (HOST\=example.com) (P  
ORT\=1521) ) ) (CONNECT_DATA\=(SID\=emrep) ) )
```

When you enter this value as the connect string, it must look like this:

```
(DESCRIPTION=(ADDRESS_  
LIST=(ADDRESS=(PROTOCOL=TCP) (HOST=example.com) (PORT=  
1521) ) ) (CONNECT_DATA=(SID=emrep) ) )
```

- b. Enter the SYSMAN password of the upgraded Management Repository that will be used by Enterprise Manager Cloud Control.
 - c. Enter the SYS password of the old Management Repository.
6. Click **Create DB Link**.

Note: If you had already provided these details and linked the two repositories, and if you are updating the connect descriptor or the SYSMAN password, then click **Re-create DB Link**.

Reconfiguring Oracle Software Library

Note: Follow these instructions only if you are upgrading using the 2-System upgrade approach.

To reconfigure an upgraded Software Library in a two-system upgrade, perform these steps:

Note:

- In a one-system upgrade, where the upgraded Enterprise Manager 12c comes up on the same host, reconfiguration is not required as the upgraded Software Library becomes functional when the system starts.

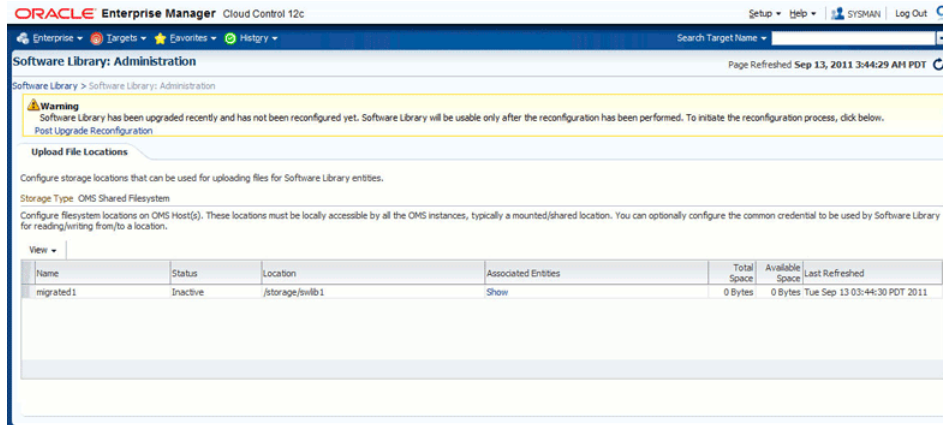
For a one system upgrade, where the upgraded Enterprise Manager 12c comes up on a different host, all the location(s) configured in the earlier, existing Enterprise Manager system for Software Library should be accessible from the new host.

- In a two-system upgrade, and sometime in a one-system upgrade on a different host, if the location configured in the earlier, existing Enterprise Manager system is a local file system path, then follow the instructions outlined in the chapter "[Upgrading with 1-System Upgrade Approach](#)" for more information.
-
-

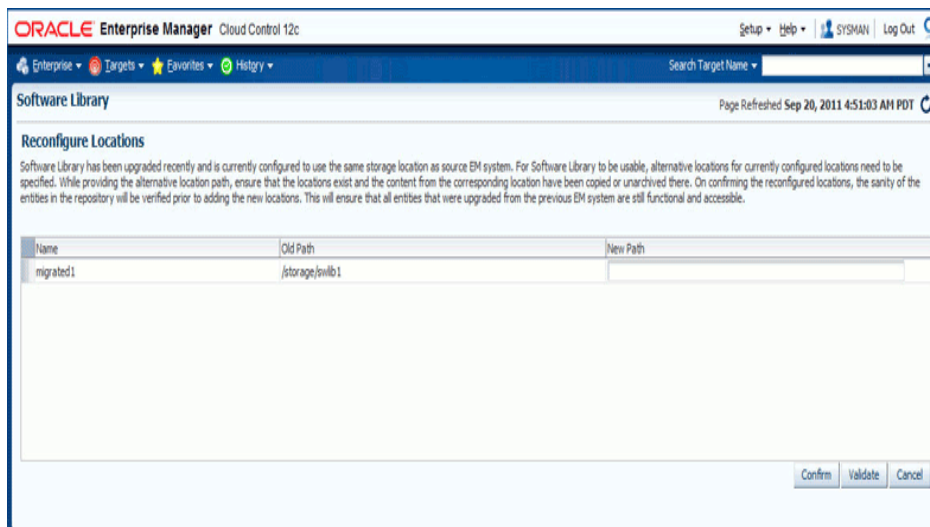
1. In Cloud Control, from **Setup** menu, select **Provisioning and Patching** and then, click **Software Library**.
2. If the Software Library has been upgraded, then on the Software Library home page, the following notification will appear:

Software Library has been upgraded recently and has not been reconfigured yet. Software Library will be usable only after the reconfiguration has been performed. To initiate the reconfiguration process, click Post Upgrade Reconfiguration.

Click **Post Upgrade Reconfiguration**, to reconfigure the Software Library.



3. On the Software Library Reconfigure Locations page, enter the new file system location that is to be configured, corresponding to the location configured in the earlier, existing Enterprise Manager system.



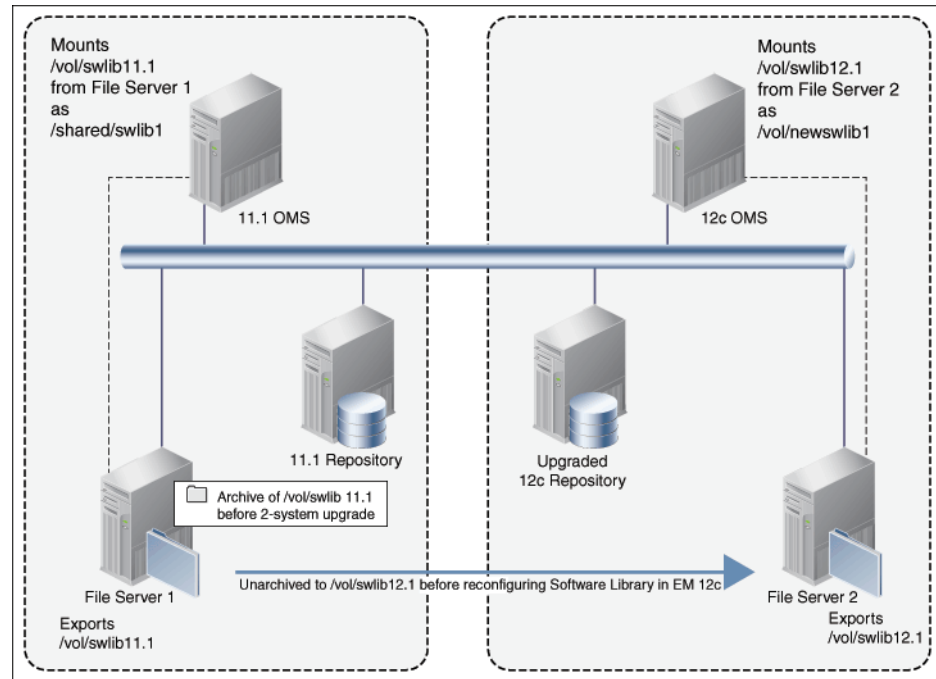
The archive of the location which was configured for the old Enterprise Manager system must be unzipped in the corresponding location on the new file system. Also, ensure that the new location, and all its unarchived files and directories have read/write permissions for the 12c OMS process owner.

For example:

In the earlier, existing Enterprise Manager system, let's assume that the Software Library was configured to use the following file system locations:

```
/shared/swlib1
/shared/swlib2
```

Figure 23–1 Two-System Reconfiguration



After an upgrade, on the Reconfigure Locations page, you will see:

```
migrated1, /shared/swlib1  
migrated2, /shared/swlib2
```

where, `migrated1` and `migrated2` are names automatically assigned to the upgraded locations.

Note: Since the new locations are only reconfiguring the OMS Shared File System storage locations, you must ensure that these new locations are either NFS-mounted shared locations or OCFS2 shared locations.

You should then provide an alternate file system path for each of the existing locations. For example, as follows:

```
migrated1, /shared/swlib1, /vol/newswlib1  
migrated2, /shared/swlib2, /vol/newswlib2
```

Before confirming this configuration, you must ensure that the new locations have the corresponding back ups of the configured Software Library directories unarchived, which means, `/vol/newswlib1` should have the same content as `/shared/swlib1`, `/vol/newswlib2` should have the same content as `/shared/swlib2` had when the backup was taken.

- a. Click **Validate** to submit a validation job that performs exhaustive validation checks on the entities being migrated. Ensure that you track this job to completion. If there are any validation errors, then it will appear on the job step. Some of the common validation errors are:
 - The new location specified for reconfiguration does not exist.

- The new location specified for reconfiguration does not have read/write permissions for the OMS process owner.

- The content of the location(s) configured in the old Enterprise Manager Software Library is not restored in the corresponding new location specified for reconfiguration.

- b.** After a successful validation, click **Confirm** to reconfigure the Software Library. A job is submitted which must be tracked to successful completion, following which you should initiate any patching or provisioning tasks.

Checking Agent Upgrade Status

Note: Perform these steps in the Enterprise Manager Grid Control console of the earlier release.

To check the status of the agent upgrade operations, follow these steps:

1. In Grid Control, click **Deployments**.
2. On the Deployments page, in the Upgrade section, click **Enterprise Manager 12c Upgrade Console**.
3. On the Upgrade Console page, do the following:
 - For macro-level details, in the Agent Upgrade Status section, view the count displayed against the following:
 - **Successful**, to identify the Management Agents that have been successfully upgraded.
 - **Failed**, to identify the Management Agents that failed to get upgraded.
 - **In Progress**, to identify the Management Agents that are currently being upgraded.
 - **Not Started**, to identify the Management Agents that are yet to be upgraded.
 - **Not Supported**, to identify the Management Agents that are not supported in the upgraded Enterprise Manager system because Oracle Management Agent 12c is not released for a particular platform.

To drill down and view more information, click the count value. Enterprise Manager Grid Control displays the Agent Upgrade Status page that provides information.

- For micro-level details, in the Other Links section, click **Agent Upgrade Status**.

On the Agent Upgrade Status page, do the following:

- To filter the list according to your needs and view only the upgrade operations that interest you, use the search functionality.

For example, to view only the deployment operations that have failed, select **Deployment** from the Operation Type list, and select **Failed** from the Operation Status list, and click **Search**.

Note: An Operation Type refers to a job submitted for a particular agent upgrade step such as *Deployment*, *Configuration*, *Health Check*, *Upgrade*, or *Switch Over*. An operation name refers to the operation name you specified while submitting any of these jobs. And each of these operations can have a status such as *Not Started*, *In Progress*, *Success*, *Not Supported*, *Failed*, or *Pending Report Verification*.

- To deploy the agent software, select one or more Management Agent from the table, and click **Deploy and Configure Agent**.

Note: You cannot deploy and configure Oracle Management Agent 12c for problematic Management Agents. To identify problematic Management Agents, see [Section 10.5](#).

Also, you can deploy and configure Oracle Management Agent 12c only on existing Management Agents that are either completely upgradable or upgradable with missing plug-ins. To identify the upgradability status of the Management Agents, see [Section 10.3](#).

- To check the health and readiness of the deployed Management Agent, select one or more Management Agents, and click **Check Agent Readiness**.
- To view the readiness check details, select one or more Management Agents, and click **View and Verify Health Check Reports**.

On the Agent Readiness Check Details page, review the reports one by one. If you want to confirm that you have verified the report, then select the Management Agent and click **Verify and Sign Off Report**. If you want to view more details about the readiness check, then select the Management Agent and click **View Detailed Report**.

- To switch over the agents, select one or more Management Agents, which have successfully been deployed, configured, and health-checked, and click **Switch Agent**.

Performing General Postupgrade Tasks

This chapter describes the postupgrade steps you must follow after upgrading to Enterprise Manager Cloud Control. In particular, this chapter describes the following postupgrade steps:

- [Performing General Postupgrade Steps](#)
- [Stopping OCM Scheduler](#)
- [Deleting Obsolete Targets](#)
- [Disabling Incident Rule Sets](#)
- [Resolving Metric Collection Errors for SOA Target](#)
- [Enabling Linux Patching After Enterprise Manager Upgrade](#)

25.1 Performing General Postupgrade Steps

Follow the postupgrade steps outlined in the chapter that describes how to install a new Enterprise Manager system, in the *Oracle Enterprise Manager Cloud Control Basic Installation Guide*.

25.2 Stopping OCM Scheduler

If OCM was installed in the Enterprise Manager system that you upgraded, then follow these steps:

- If you upgraded from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5.0), then follow these steps:
 1. Set the environment variable `ORACLE_HOME` to the Oracle Management Service (OMS) home.
 - In bash terminal, run the following command:

```
export ORACLE_HOME=<absolute_path_to_oms_home>
```
 - In other terminals, run the following command:

```
setenv ORACLE_HOME <absolute_path_to_oms_home>
```
 2. Stop the OCM scheduler:

```
$ORACLE_HOME/ccr/bin/emCCR stop
```

Note: If you have the OCM scheduler installed on Oracle Management Agent, then repeat these steps on the Management Agent home as well. In this case, set the environment variable `ORACLE_HOME` to the Management Agent home as described in Step (1), and perform Step (2) from its home.

- If you upgraded from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1.0), then
 1. Set the environment variable `ORACLE_CONFIG_HOME` to the OMS instance home:
 - In bash terminal, run the following command:


```
export ORACLE_CONFIG_HOME=<absolute_path_to_gc_inst>
```
 - In other terminals, run the following command:


```
setenv ORACLE_CONFIG_HOME <absolute_path_to_gc_inst>
```
 2. Set the environment variable `ORACLE_HOME` to the OMS home:


```
setenv ORACLE_HOME <absolute_path_to_oms_home>
```
 3. Stop the OCM scheduler:


```
​$ORACLE_HOME/ccr/bin/emCCR stop
```

Note: If you have the OCM scheduler installed on Oracle Management Agent, then repeat these steps on the Management Agent home as well. In this case, skip Step (1), set the environment variable `ORACLE_HOME` to the Management Agent home as described in Step (2), and perform Step (3) from its home.

25.3 Deleting Obsolete Targets

The following targets from the earlier release of Enterprise Manager are not deleted automatically. This is because you might have created notification rules, metric threshold settings, compliance standard settings, jobs, and so on for these targets, and you might want to copy them to the new Oracle WebLogic Server targets of Enterprise Manager Cloud Control. After copying them, manually delete these targets.

- While upgrading from Enterprise Manager 10g Grid Control Release 5 (10.2.0.5), the following targets are not deleted automatically. You must delete them manually.
 - EM Website
 - EM Website System
 - The following targets of each old OMS. You can delete these by deleting the top-level Oracle Application Server target of each old OMS.
 - * Oracle Application Server
 - * OC4J
 - * Oracle HTTP Server
 - * Web Cache

- While upgrading from Enterprise Manager 11g Grid Control Release 1 (11.1.0.1), the following targets are not deleted automatically. You must delete them manually.
 - EM Website
 - EM Website System
 - The following targets of each old OMS. You can manually delete these by deleting the top-level farm target `secFarm_GCDomain`.
 - * Oracle Fusion Middleware Farm
 - * Oracle Weblogic Domain
 - * Application Deployment
 - * Metadata Repository

Note: After you upgrade your Enterprise Manager using the 1-System upgrade approach, these targets might appear as they are up and running. This status is unreal and incorrect. In any case, do not investigate to resolve the status issue. Manually delete the targets as they are no longer needed in the Enterprise Manager Cloud Control.

25.4 Disabling Incident Rule Sets

If you upgraded using the 2-System upgrade approach, then disable the default incident rule sets. If you do not disable them, the incidents are automatically created for all critical metric alerts.

To disable the default incident rule sets, follow the steps:

1. In Cloud Control, from the **Setup** menu, select **Incidents**, and then select **Incident Rules**.
2. On the Incident Rules - All Enterprise Rules page, scroll down the table, and expand **Incident management Ruleset for all targets**.
3. Select the row for the rule set you want to disable.
4. From the **Actions** menu, click **Disable**.
5. On the pop-up window, click **OK**.
6. Repeat Step (3) to Step (5) for every rule set you want to disable.
7. Once all the rule sets are disabled, ensure that the **Enabled** column of the table shows *No* with a warning icon next to it.

25.5 Resolving Metric Collection Errors for SOA Target

If you were monitoring a SOA target in your earlier release of Enterprise Manager, then in the health report you generated in [Chapter 12](#), you might have seen metric collection errors for the metrics *Top SOA SQL Queries* and *Dehydration Store Tables*.

To resolve that issue, access the Monitoring Configuration page of the SOA target, and provide the database credentials.

25.6 Enabling Linux Patching After Enterprise Manager Upgrade

After upgrading Enterprise Manager, you must stop all active jobs for Linux patching that were submitted prior to the upgrade, and resubmit them on the same targets. This section describes how you can achieve this.

In particular, this section covers the following:

- [Configuring DownloadLatestPackages Job](#)
- [Configuring UpdateHostPackages Job](#)

25.6.1 Configuring DownloadLatestPackages Job

To configure the DownloadLatestPackages job, follow these steps:

1. Stop active jobs which were scheduled prior to upgrade as follows:
 - a. From the Enterprise menu, select **Job** and then **Activity**. The Job Activity page is displayed.
 - b. In the Job Activity page, click the **Advanced Search** link.
 - c. In the Advanced Search options, select Job Type as **DownloadLatestPkgs**, Target Type as **Host**, Status as **Active**, Scheduled Start as **All**, and then click **Go**.
 - d. In the Advanced Search result, select each job listed in the table and click **Stop**.
2. For each host target on which an active **DownloadLatestPkgs** job was stopped, resubmit a new **DownloadLatestPkgs** job on it as follows:
 - a. From the **Setup** menu, select **Provisioning and Patching** and then **Linux Patching**. The Patching Setup page is displayed.
 - b. In the Patching Setup page, click **Setup RPM Repository**.
 - c. In the Setup RPM Repository page, select the Host target and set Normal Host Credentials and Privileged Host Credentials for this host target.
 - d. Click **Apply** to submit the new job.

25.6.2 Configuring UpdateHostPackages Job

To configure the UpdateHostPackages job, follow these steps:

1. Stop active jobs which were scheduled prior to upgrade as follows:
 - a. From the Enterprise menu, select **Job** and then **Activity**. The Job Activity page is displayed.
 - b. In the Job Activity page, click the **Advanced Search** link.
 - c. In the Advanced Search options, select Job Type as **UpdateHostPackages**, Target Type as **All Target Types against which jobs were submitted**, Status as **Active**, Scheduled Start as **All**, and then click **Go**.
 - d. In the Advanced Search result, select each job listed in the table and click **Stop**.
2. For each group target on which an active **UpdateHostPackages** job was stopped, resubmit a new **UpdateHostPackages** job on it as follows:
 - a. From the **Setup** menu, select **Provisioning and Patching** and then **Linux Patching**.

- b. In the Patching Setup page, click **Setup Groups**. The Setup Groups page is displayed.
- c. In the Setup Groups page, select the group on which you stopped an active UpdateHostPackages job and click **Edit**. The Edit Group wizard is displayed.
- d. In the Edit Group: Properties page, click **Next**.
- e. In the Edit Group: Package Repositories page, click **Next**.
- f. In the Edit Group: Credentials page, either use Host Preferred Credentials or Override Preferred Credentials and specify Normal Host Credentials and Privileged Host Credentials. Click **Next**.

Note: Before editing this step, ensure that the host Preferred credentials are set already or the appropriate Named Credentials have been created already. If not, from the **Setup** menu, select **Security** and then **Named Credentials** to create Named Credentials or **Preferred Credentials** to set the Preferred Credentials for the host targets contained in the Linux Patching group.

- g. In the Edit Group: Review page, click **Finish** to submit the new job.

Tracking the Status of Deferred Data Migration Jobs

This chapter describes the following:

- [Overview of Deferred Data Migration](#)
- [Tracking the Status of Deferred Data Migration Jobs](#)

26.1 Overview of Deferred Data Migration

Deferred Data Migration is a post-upgrade activity to migrate the format of the data stored in an earlier release of Enterprise Manager to the format compatible with the upgraded Enterprise Manager system. The migration activity is essentially a job in Enterprise Manager that is submitted when the Oracle Management Repository gets upgraded and is scheduled to run in the background when the upgraded Enterprise Manager system starts functioning.

The format of the data stored in Enterprise Manager Cloud Control is different from the format in which the data was stored in any earlier release of Enterprise Manager.

When you upgrade from an earlier release of Enterprise Manager to Enterprise Manager Cloud Control, the data format gets automatically converted or migrated to the format that is compatible with Enterprise Manager Cloud Control.

However, the time taken to migrate the data format depends on the volume of data available in your earlier release of Enterprise Manager. Therefore, if you have a large amount of data, then it takes longer to migrate, and as a result, the upgrade process takes more time to complete. Unfortunately, until the upgrade process completes, your existing Enterprise Manager system might be unavailable, particularly when you use a 1-System upgrade approach (either on the local host or on a different, remote host).

Considering this, Oracle has fine-tuned its upgrade process to migrate the data format in two distinct phases.

In the first phase, when the Enterprise Manager system is shut down and upgraded, the most critical data relevant to the functioning of Enterprise Manager Cloud Control is migrated within a short time so that the new system can start functioning without much downtime. At this point, only some historical data is unavailable, but you can start monitoring the targets in the upgraded Enterprise Manager system, and see new alerts generated by the upgraded Oracle Management Agent.

In the second phase, after the upgraded Enterprise Manager system starts functioning, the remaining data is migrated.

The data whose format is migrated in the second phase, after Enterprise Manager Cloud Control starts functioning, is called the *Deferred Data*, and this process of migrating from old to new format is called the *Deferred Data Migration*.

Note: If you want to prevent the DDMP jobs from running immediately by default, then see [Chapter 7](#) and [Chapter 8](#) (Step 6).

26.2 Tracking the Status of Deferred Data Migration Jobs

To track the status of deferred data migration jobs, follow these steps:

1. In Cloud Control, from the **Setup** menu, click **Post Upgrade Tasks**.
2. On the Post Upgrade Tasks page, click the **Deferred Data Migration** tab.

The tab provides a list of data migration jobs with their status, start date and time, and end date and time.

3. In this tab, you can do the following:
 - To start a data migration job for a component, select that component and click **Start**. By default, the job starts immediately. You cannot change this behavior.
 - To rerun a failed job, click the status icon to reach the Job Run page. On the Job Run page, click **Edit**. On the Edit <JobName> Job page, click **Submit** to rerun the job.
 - To hide or unhide the table columns, from the **View** list, select an appropriate option.
 - To detach the table from the screen, click **Detach**.

Tracking the Status of Accrued Data Migration Jobs

Note: This chapter is applicable only for 2-System upgrade approach.

This chapter describes the following:

- [Overview of Accrued Data Migration](#)
- [Tracking the Status of Accrued Data Migration Jobs](#)

27.1 Overview of Accrued Data Migration

Accrued Data Migration is a post-upgrade activity to migrate the accrued data stored in an earlier release of Oracle Management Repository (Management Repository) to the upgraded Management Repository. The accrued data relates to functional areas such as blackouts, alerts, events, metrics, and so on.

Note: The Accrued Data Migration Process does not migrate any manually created data such as new job type, user-defined metrics, Software Library-related changes, and so on.

The migration activity is essentially a job in Enterprise Manager that runs in the background immediately after the earlier releases of Oracle Management Agents (Management Agents) are switched over to Oracle Management Agent 12c, particularly in the case of 2-System upgrade approach.

As part of the upgrade process, when you switch over the earlier releases of Oracle Management Agents to Oracle Management Agent 12c, the new Management Agents start communicating with Enterprise Manager Cloud Control, and start uploading data to the upgraded Oracle Management Repository (Management Repository).

In the 1-System upgrade approach, the entire Enterprise Manager system is upgraded, and therefore, all the Management Agents are switched over at a given time. In this approach, earlier releases of Management Agents cannot coexist with the upgraded ones, and once they are switched over, the upgraded Management Agents upload data only to one Management Repository at any given point, which is the upgraded repository. Therefore, there is no scope for accrued data.

However, in the 2-System upgrade approach, you can choose to switch over your Management Agents in phases. When one set of Management Agents are switched

over, they start uploading data about their hosts and targets to the upgraded Management Repository, whereas the ones that are not switched over yet, continue to upload data about their hosts and targets to the old Management Repository. Therefore, the earlier releases of Management Agents coexist with the upgraded ones when only some of them are switched over, and under such circumstances, the data is uploaded to the old Management Repository as well as the new one at a given point. However, note that only one Management Agent represents a host at any given time, so the coexistence does not indicate two Management Agents on the same host. It only indicates an earlier release of Management Agent monitoring a host that coexists with an upgraded Management Agent monitoring another host.

When you switch over the next set of Management Agents in the next phase, although they start uploading data to the upgraded Management Repository, the data uploaded to the old Management Repository before being switched over continues to exist in the old Management Repository. This data is called the *Accrued Data*, and the process of migrating this accrued data from the old Management Repository to the new one is called the *Accrued Data Migration Process*.

Note: The accrued data migration jobs migrate ECM history data with the following exceptions:

- If the ECM history data is associated with a target that is no longer part of the Enterprise Manager system, then the ECM history data for that target is not migrated to Enterprise Manager Cloud Control.
- For Oracle WebLogic Server targets, the WebLogic configuration data is not migrated. This configuration data has changed significantly in Enterprise Manager Cloud Control.
- As part of the data migration process, summary counts are now calculated and displayed in the ECM Summary region. For migrated data, the summary counts are only calculated for the last seven days.

If you do not see key values that you saw in the past, or if you see new values as key values, then note that this is an expected behavior. Some snapshots have had metadata changes in the last release and key values have changed. If metadata keys were removed from the metadata, those values will no longer be displayed in the Enterprise Manager Cloud Control as key columns, though the data is still present in the migrated database. If existing columns are now flagged as key columns, those columns will start appearing as key columns for newly collected data only. For new columns that are added either as key columns or non key columns, data will start appearing for newly collected data only.

Note: If you want to prevent the ADMP jobs from running immediately by default, then see [Chapter 8](#) (Step 6).

27.2 Tracking the Status of Accrued Data Migration Jobs

To track the status of accrued data migration jobs, follow these steps:

1. In Cloud Control, from the **Setup** menu, click **Post Upgrade Tasks**.

2. On the Post Upgrade Console page, click the **Accrued Data Migration** tab.

The Accrued Data Migration page displays information about the accrued data migration jobs related to all the targets available in your Enterprise Manager system. By default, for every target, the accrued data migration job migrates the ECM history details as well as the metric details.

3. In this tab, you can do the following:

- To control the data being migrated for all the targets, from the **Run accrued data migration for** list, select one of the following options:
 - **ECM HISTORY MIGRATION**, to migrate only the ECM history details.
 - **METRIC DATA MIGRATION**, to migrate only the metric details.
 - **All**, to migrate the ECM history details as well as the metric details.
- To view different types of data, from the **View Targets** list, select one of the following options:
 - **All**, to view all the accrued data migration jobs for all the targets in your Enterprise Manager system.
 - **Active**, to view the accrued data migration jobs that either failed or are currently running.
 - **History**, to view the accrued data migration jobs that succeeded.
 - **Not Started**, to view the accrued data migration jobs that have not started yet.
- To retry a failed job, select the target for which the job failed and click **Retry**.
- To stop a running job, select the target for which you want to stop the job and click **Stop**.

Generating and Viewing Diff Reports

Note: This chapter is applicable only for 2-System upgrade approach.

This chapter describes the following:

- [Overview of Diff Reports](#)
- [Generating and Viewing Diff Reports](#)

28.1 Overview of Diff Reports

Diff Reports provide information about the configuration or setup-related changes that were manually made to the earlier release of Enterprise Manager while it was being upgraded to Enterprise Manager Cloud Control using the 2-System upgrade approach.

In the 2-System upgrade approach, the earlier release of Enterprise Manager coexists with Enterprise Manager Cloud Control until the upgrade operation ends. In some production environments, the upgrade operation might take a long time to complete due to a large volume of data, and during this period, you might make some changes to the functional areas in the earlier release. For example, you might configure an additional location for the software library.

Such changes must be carried over to Enterprise Manager Cloud Control so that the upgraded system is identical to the earlier release. The Diff Reports show a summary of such changes so that you can manually redo those changes in Enterprise Manager Cloud Control.

28.2 Generating and Viewing Diff Reports

To generate and view diff reports, follow these steps:

1. In Cloud Control, from the **Setup** menu, click **Post Upgrade Tasks**.
2. On the Post Upgrade Console page, click the **Diff Report** tab.

The Diff Report page lists the reports that were generated in the past for various components. However, when you visit this page the first time, you will not see any reports.

3. On this page, you can do the following:
 - To generate the reports for various components, click **Regenerate Report**.

Note: On clicking **Regenerate Report**, the status in the Status column changes to *In Progress*. Keep refreshing the page manually until the status changes to *Completed*.

- To view a report of a particular component, select a component (row) from the table, and click **Show Report**.
- To refresh a report and view the latest changes related to a component, select a component (row) from the table, and click **Regenerate Report**.
- To hide or unhide the table columns, or to reorder the table columns, from the **View** list, select an appropriate option.
- To detach the table from the screen, click **Detach**.

Viewing Inactive Targets in the Upgraded Enterprise Manager System

Note: This chapter is applicable only for 2-System upgrade approach.

Targets available in the existing Enterprise Manager system are active (monitored) in the upgraded Enterprise Manager system only when the Oracle Management Agents that were monitoring those targets are switched over to the upgraded Enterprise Manager system using Oracle Management Agent 12c.

To view a list of targets that are currently inactive in the upgraded Enterprise Manager system, follow these steps:

1. In Cloud Control, from the **Setup** menu, click **Post Upgrade Tasks**.
2. On the Post Upgrade Console page, click the **Targets with Pending Activation** tab.
3. In this tab, you can view a list of inactive targets.

To search for targets of your choice, enter a keyword or a part of the target name (or target type) in the search text box placed right above the Target Name column (or Target Type column).

Alternatively, you can click the links in the **Refine Search** pane to filter the table and list the targets of your choice.

Note: To convert these inactive targets to active targets, switch over the Management Agents that are monitoring these targets in the existing Enterprise Manager system to the upgraded Enterprise Manager system. For information about switching over the Management Agents, see [Chapter 14](#).

Signing Off Accrued Data Migration Process

Note: This chapter is applicable only for 2-System upgrade approach.

After you switch over the Oracle Management Agents (Management Agent) to the Enterprise Manager Cloud Control, you can deinstall the earlier release of Management Agents. Instead of manually deinstalling the Management Agents, you can formally sign off the Accrued Data Migration Process (ADMP) for each of the Management Agents and have the Post Upgrade Console automatically deinstall them for you.

To sign off the ADMP process for each of the Management Agents, follow these steps:

1. In Cloud Control, from the **Setup** menu, click **Post Upgrade Tasks**.
2. On the Post Upgrade Tasks page, click the **Sign Off** tab.
3. In this page, you can do the following:
 - To search Management Agents for which you have signed off the ADMP process, for which you are yet to sign off, or for which you are in the process of signing off, do the following:
 - (i) From the **Search Criteria** list, select an appropriate option.
 - (ii) In the **Agent Name** field, enter the name of the Management Agent. You can leave this blank if you want to search all Management Agents with a particular sign-off status. Alternatively, you can enter a part of the name and use wildcards to search for Management Agents with a similar name.
 - (iii) Click **Search**.

Note: If you have not run the accrued data migration job for a Management Agent, then you cannot search and sign off that Management Agent. You will not find that Management agent even if you try searching for it using the search conditions.

- To select Management Agents and formally sign off the ADMP process for each of them, do the following:
 - (i) In the table, select the Management Agents you want to sign off. To select all the Management Agents, select **Select All**.
 - (ii) Click **Sign Off Migration**.

(iii) Provide credentials to access the hosts on which the selected Management Agents were running.

(iv) Click **OK**.

Note: Once you sign off, the selected old Management Agents will automatically be deinstalled and removed, and they cannot be recovered in any way. Therefore, before you sign off, ensure that your Management Agents have switched over successfully and they are fully functional, and their targets are successfully being monitored in Enterprise Manager Cloud Control.

- To hide or unhide the table columns, from the **View** list, select an appropriate option.
- To detach the table from the screen, click **Detach**.

Updating Incident Rules

During upgrade, all *Notification Rules* created in the earlier release of Enterprise Manager are automatically migrated to corresponding *Incident Rulesets* that act on the targets originally defined in the *Notification Rule*. For more information about *Incident Rulesets*, see [Appendix A](#).

However, for situations where the target type modeling has changed in Enterprise Manager Cloud Control, you must manually adjust the rules. This appendix describes how you can manually adjust the rulesets.

In particular, it covers the following:

- [Why Update Incident Rules](#)
- [Updating Incident Rules for Moved Metrics](#)
- [Updating Incident Rules for Renamed Metrics](#)
- [Deleting Incident Rules](#)

31.1 Why Update Incident Rules

In the earlier releases of Enterprise Manager, *OMS and Repository* was a common target type defined for all the OMSes in your environment. And the metrics collected for the different OMSes were shown within this common target type.

However, in Enterprise Manager Cloud Control, in addition to the target type *OMS and Repository*, a new target type *Oracle Management Service* has been introduced to represent each of the OMSes in your environment. Therefore, if you have five OMSes in your environment, you will see one target type *OMS and Repository* and five instances of the target type *Oracle Management Service* - one for each OMS.

While the target type *OMS and Repository* captures metrics that are common to all the OMSes in your environment, the target type *Oracle Management Service* captures metrics specific to an OMS.

[Table 31-1](#) lists the metrics and describes the changes done to them due to the introduction of a new target type *Oracle Management Service*, and the actions you must take for each change.

Table 31–1 Changes to Metrics and Updates to Be Done

Change Type	Change Description	Affected Metrics	Action to Be Taken by You
Retained	Some metrics have been retained for the same target type— <i>OMS and Repository</i> .	The following metrics have been retained: <ul style="list-style-type: none"> ■ Collections Waiting To Run ■ DBMS Job Invalid Schedule ■ DBMS Job Processing Time (% of Last Hour) ■ DBMS Job UpDown ■ Dequeue Status ■ Enqueue Status ■ Job Step Backlog ■ Notification UpDown ■ Number of Active Agents ■ Overall Files Pending Load - Agent ■ Overall Rows Processed by Loader in the Last Hour ■ Number of Agent Restarts ■ Target Addition Rate (Last Hour) ■ User Addition Rate (Last Hour) 	No changes required.
Moved	Some metrics have been moved to the individual target type— <i>Oracle Management Service</i> .	The following metrics have been moved: <ul style="list-style-type: none"> ■ Loader Throughput (rows per second) ■ Total Loader Runtime in the Last Hour (seconds) ■ Management Service Status ■ Job Dispatcher Processing Time, (% of Last Hour) ■ Service Status ■ Repository Session Count <p>[Note: This metric has moved under the child targets <i>OMS Console</i> and <i>OMS Platform</i>]</p>	Set up new incident rules to respond to the metrics that have been moved to different target types. See Section 31.2
Renamed	Some metrics have been renamed for easy understanding.	The following metrics have been renamed: <ul style="list-style-type: none"> ■ Average Notification Delivery Time (ms) Per Method [Renamed to Average Notification Time (seconds)] ■ Notifications Waiting [Renamed to Pending Notifications Count] 	Update the incident rules set to the metrics that have been renamed. See Section 31.3

Table 31–1 (Cont.) Changes to Metrics and Updates to Be Done

Change Type	Change Description	Affected Metrics	Action to Be Taken by You
Decommissioned	Some metrics have been decommissioned due to lack of support in Enterprise Manager Cloud Control.	<p>The following metrics have been decommissioned:</p> <ul style="list-style-type: none"> ■ Number of Duplicate Targets ■ Notification Processing Time (% of Last Hour) ■ Overall Files Pending Load - Loader ■ Notifications Waiting <p>(Note: This is different from the Notifications Waiting metric that is renamed. This one does not have objects, while the one renamed has objects.)</p>	Remove decommissioned metrics from the incident rules. See Section 31.4

31.2 Updating Incident Rules for Moved Metrics

To update the incident rules set to the metrics that have been moved to the individual target type *Oracle Management Service* in Enterprise Manager Cloud Control, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Incidents**, and then, click **Incident Rules**.
2. On the Incident Rules page, from the table, select an incident rule created for Oracle Management Service (OMS), click **Edit**.
3. On the Edit Rule Set page, in the Rules tab, select the event rule that operates on the moved metrics, and click **Edit**.

Enterprise Manager displays the Edit Rule Wizard where you can edit the incident rule for the selected incident rule set.

4. In the Edit Rule Wizard, do the following:
 - a. On the Select Events page, select the metrics listed in the second row of [Table 31–1](#), and click **Remove**.
 - b. Click **Next**.
 - c. On the Add Actions page and the Specify Name and Description page, click **Next** without making any change.
 - d. On the Review page, click **Continue**.

5. Click **Save**.

Enterprise Manager displays the Incident Rules page.

6. On the Incident Rules page, click **Create Rule Set**.
7. On the Create Rule Set page, enter a unique name for the rule set.
8. In the Targets tab, select **All targets of types**, and select **Oracle Management Service**.
9. In the Rules tab, click **Create**.
10. In the Select Type of Rule to Create dialog, select **Event Rule**, and click **Continue**.

Enterprise Manager displays the Create New Rule Wizard where you can create a new incident rule set.

11. In the Create New Rule Wizard, do the following:
 - a. On the Select Events page, from the **Event Type** list, select **Metric Alert**.

Note: For the metric *Management Service Status*, select **Target Availability** from the **Event Type** list.

 - b. Select **Specific metric alerts**, and click **Add**.
 - c. In the Select Specific Metric Alert dialog, do the following:
 - a. In the Search region, from the **Target Type** list, select **Oracle Management Service**, and then, click **Search**.
 - b. From the table, select the moved metrics listed in the second row of [Table 31-1](#).
 - c. In the Severity and Corrective Action Status region, from the **Severity** list, select an appropriate severity level.
 - d. Click **OK**.
 - d. Click **Next**.
 - e. On the Add Actions page and the Specify Name and Description page, click **Next** without making any change.
 - f. On the Review page, click **Continue**.
12. Click **Save**.

Enterprise Manager displays the Incident Rules page.

Note: Repeat the procedure for all other incident rules created for the OMS.

31.3 Updating Incident Rules for Renamed Metrics

To update the incident rules set to the metrics that have been renamed in Enterprise Manager Cloud Control, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Incidents**, and then, click **Incident Rules**.
2. On the Incident Rules page, from the table, select an incident rule created for Oracle Management Service (OMS), click **Edit**.
3. On the Edit Rule Set page, in the Rules tab, select the event rule that operates on the renamed metrics, and click **Edit**.

Enterprise Manager displays the Edit Rule Wizard where you can edit the incident rule for the selected incident rule set.

4. In the Edit Rule Wizard, do the following:
 - a. On the Select Events page, select the metrics listed in the third row of [Table 31-1](#), and click **Remove**.
 - b. Click **Add**.

- c. In the Select Specific Metric Alert dialog, do the following:
 - a. In the Search region, from the **Target Type** list, select **OMS and Repository**, and then, click **Search**.
 - b. From the table, select the renamed metrics listed in the third row of [Table 31-1](#).
 - c. In the Severity and Corrective Action Status region, from the **Severity** list, select an appropriate severity level.
 - d. Click **OK**.
- d. Click **Next**.
- e. On the Add Actions page and the Specify Name and Description page, click **Next** without making any change.
- f. On the Review page, click **Continue**.

Note: Repeat the procedure for all other incident rules created for the OMS.

31.4 Deleting Incident Rules

To remove the decommissioned metrics from the the incident rules, follow these steps:

1. In Cloud Control, from the **Setup** menu, select **Incidents**, and then, click **Incident Rules**.
2. On the Incident Rules page, from the table, select an incident rule created for Oracle Management Service (OMS), click **Edit**.
3. On the Edit Rule Set page, in the Rules tab, select the rule *Metric Alerts Event Rule*, and click **Edit**.

Enterprise Manager displays the Edit Rule Wizard where you can edit the incident rule for the selected incident rule set.

4. In the Edit Rule Wizard, do the following:
 - a. On the Select Events page, select the metrics listed in the last row of [Table 31-1](#), and click **Remove**.
 - b. Click **Next**.
 - c. On the Add Actions page and the Specify Name and Description page, click **Next** without making any change.
 - d. On the Review page, click **Continue**.

Note: Repeat the procedure for all other incident rules created for the OMS.

Part VII

Appendixes

This part contains the following appendixes:

- [Appendix A, "Overview of Notification in Enterprise Manager Cloud Control"](#)
- [Appendix B, "Overview of Metric Changes in Enterprise Manager Cloud Control"](#)
- [Appendix C, "Identifying Jobs That Will Not Run in the Enterprise Manager System"](#)
- [Appendix D, "Meeting Prerequisites for Installing Oracle Management Agent"](#)
- [Appendix E, "Updating Server Load Balancer Configuration Settings"](#)
- [Appendix F, "Setting Preferred Credentials Using EMCLI"](#)
- [Appendix G, "Searching and Adding Oracle Management Agents"](#)

Overview of Notification in Enterprise Manager Cloud Control

Prior to Enterprise Manager Cloud Control, the notification system notified administrators of target availability status changes, metric alerts, and status changes of job executions. In addition to notifying the administrators, the notification system performed actions such as running operating system commands, including scripts, and PL/SQL procedures when an alert was triggered.

This appendix describes how the notification system has changed significantly in Enterprise Manager Cloud Control. In particular, this appendix covers the following:

- [Understanding Events, Incidents, and Incident Rulesets](#)
- [Accessing Incident Rulesets](#)
- [Migrating Notification Rules to Incident Rulesets](#)
- [Working with Notification Methods and Actions](#)

A.1 Understanding Events, Incidents, and Incident Rulesets

In the earlier releases of Enterprise Manager, the notification system operated using *Notification Rules*, which were a set of predetermined rules or conditions indicating when a notification had to be sent and what actions had to be taken.

In Enterprise Manager Cloud Control, this concept of *Notification Rules* has been enhanced and subsumed into a much larger and newer concept called *Incident Rulesets*.

Before discussing *Incident Rulesets*, understand the concept of *Events* and *Incidents*.

- *Events* are significant and interesting occurrences in your managed environment. Target availability status changes, metric alerts, and status changes of job executions are examples of the types of events that Enterprise Manager detects. Users may be interested in getting notified about these events and responding accordingly to resolve the underlying issues. By formalizing the concept of events, Enterprise Manager extends the monitoring functionality to additional occurrences in the enterprise that might be of interest, such as metric evaluation errors or compliance standard violations.
- *Incidents* are a subset of related events that may indicate potential or actual disruption to the dependent IT services, and require attention from an administrator or a team. *Incidents* can be created for such events, which can then be assigned to an administrator and tracked to completion.

Incident Ruleset is a set of rules that typically operate on a set of targets, and include individual rules to notify appropriate personnel and take appropriate action on events, incidents, and problems.

Note: For information about the problems, refer to the *Oracle Enterprise Manager Administrator's and User's Guide* available in the Enterprise Manager documentation library at:

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

A rule can operate on events to send notifications as well as create incidents. It can also operate on specific incidents, so you can auto-assign, prioritize, or even escalate them via time-based conditions.

Incident Rulesets are further classified into enterprise and private rulesets.

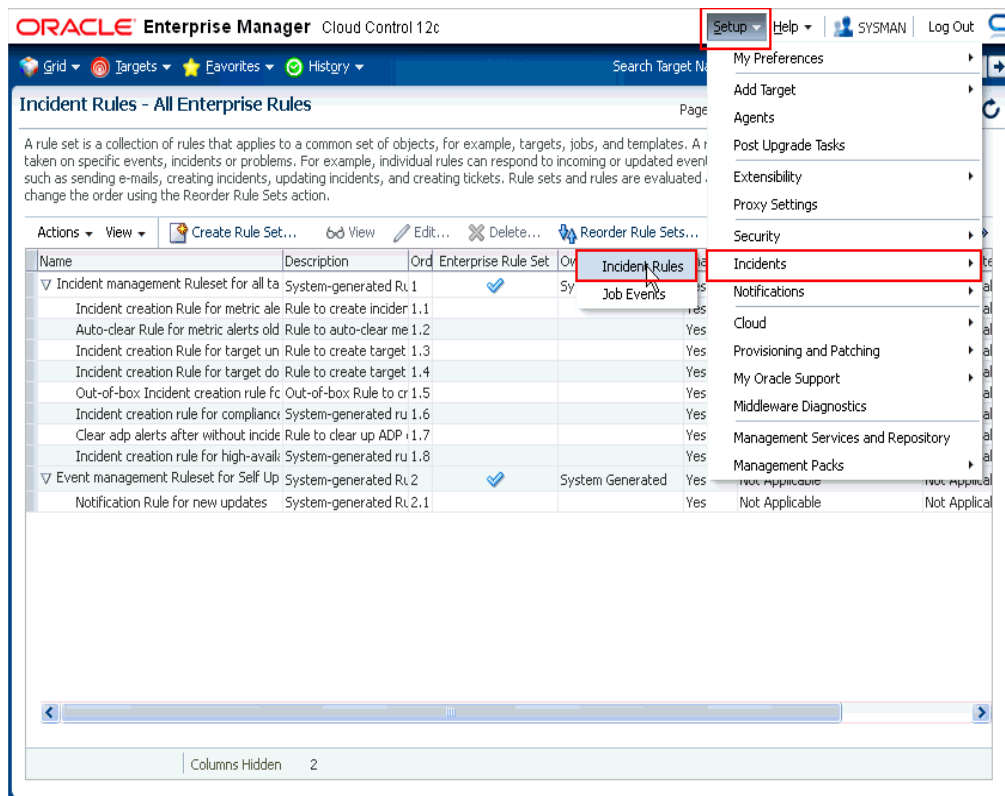
- *Enterprise Rulesets* are used to automate and enforce enterprise level behavior such as notifying one or more users, sending notifications using advanced notification methods, raising tickets in external ticketing systems, creating and updating incidents. Only administrators with the *Create Enterprise Ruleset* privilege can create these rulesets.
- *Private Rulesets* are useful for administrators to e-mail themselves about specific changes. They can be created by any administrator and can only be used to send e-mails to the owner of the ruleset.

All *Incident Rulesets* can be edited by the owner of the ruleset and any super administrator. In addition, the owners can designate other users as coauthors of *Enterprise Rulesets*. This enables shared management of the ruleset.

A.2 Accessing Incident Rulesets

To view all *Incident Rulesets*, in Enterprise Manager Cloud Control, from the **Setup** menu, click **Incidents**, and then, select **Incident Rules**. [Figure A-1](#) shows the Incident Ruleset page:

Figure A-1 Viewing Incident Rulesets



A.3 Migrating Notification Rules to Incident Rulesets

During upgrade, all *Notification Rules* created in the earlier release of Enterprise Manager are automatically migrated to corresponding *Incident Rulesets* that act on the targets originally defined in the *Notification Rule*.

The following *Notification Rules* are migrated to *Enterprise Rulesets*:

- *Notification Rules* that send e-mails to owners who have not created the rules
- *Notification Rules* that invoke an advanced notification method

The following *Notification Rules* are migrated to *Private Rulesets*:

- *Notification Rules* that have no actions.
- *Notification Rules* that send e-mails to owners who have created the rules.

Each of the three possible criteria—availability, metrics, jobs—defined in an old *Notification Rule* are migrated to three individual rules that operate on appropriate events. The action defined at the *Notification Rule* level is copied over to each of these rules.

One exception is that the concept of Policy Violations is being withdrawn in Enterprise Manager Cloud Control, and therefore, all policy-specific criteria are ignored and none of the rules that solely operate on policies are migrated.

The owners of *Notification Rules*, which were created in the earlier release of Enterprise Manager, become the owners of the corresponding *Incident Rulesets* in Enterprise Manager Cloud Control. These owners can edit the *Enterprise Rulesets* and *Private*

Rulesets. In addition, all administrators can create *Private Rulesets* to send e-mails to themselves.

Going forward, the super administrators should determine which administrators can create *Enterprise Rulesets* by granting the *Create Enterprise Ruleset* resource privilege.

Note: For situations where the target type modeling has changed in Enterprise Manager Cloud Control, you must manually adjust the rules as described in [Chapter 31](#).

A.4 Working with Notification Methods and Actions

Notification methods and actions defined in earlier releases of Enterprise Manager will continue to work in Enterprise Manager Cloud Control, and the input to these original notification methods are backward compatible in Enterprise Manager Cloud Control. So if you had an OS command or a PL/SQL notification method that operated on metric alerts, you will continue to receive the same input after upgrade. However, all new notification methods you create in Enterprise Manager Cloud Control will accept input based on the new event and incident model.

Note: Oracle strongly recommends you to replace the Notification Methods created in the earlier releases of Enterprise Manager with the new Enterprise Manager Cloud Control-specific notification methods that operate on the new event model. With the next major release of Enterprise Manager Cloud Control, the older notification methods will no longer function.

Overview of Metric Changes in Enterprise Manager Cloud Control

This appendix describes the changes to the metrics of the following targets:

- [Oracle SOA Infrastructure](#)
- [Oracle SOA Composite](#)
- [Oracle Service Bus](#)
- [Oracle WebLogic Server](#)
- [JBoss Application Server](#)
- [Siebel Enterprise](#)
- [Siebel Server](#)

B.1 Oracle SOA Infrastructure

The following are the changes to the metrics related to Oracle SOA Infrastructure:

- The old metric *SOA Infrastructure - Service Engine Detail Metrics* appears on the *All Metrics* page to show historical data. However, there is no further collection for this metric.
- The new metric *SOA Infrastructure - Service Engine Detail Metrics* has now moved under the target component type **SOA Infrastructure Engine**.
- In addition, the following metrics have been introduced:
 - *Top SOA SQL Queries*
 - *Dehydration Store Tables*
- In the *Enterprise Manager 12c Upgrade Console*, when you generate a health report, you might see metric collection errors for the new metrics. You can ignore these errors and proceed further. However, ensure that you provide the database credentials for this target as described in [Chapter 25](#).

B.2 Oracle SOA Composite

The following are the changes to the metrics related to Oracle SOA Composite:

- The old metrics *SOA Composite - Component Detail Metrics* and *SOA Composite - Services/References Detail Metrics* appear on the *All Metrics* page to show historical data. However, there is no further collection for this metric.

- The new metric *SOA Composite - Component Detail Metrics* has now moved under the target component type **SOA Composite Component**.
- The new metric *SOA Composite - Services/References Detail Metrics* has now been divided into the following metrics:
 - *SOA Composite Service Metric* that appears under the target component type **SOA Composite Service**.
 - *SOA Composite Reference Metric* that appears under the target component type **SOA Composite Reference**.

B.3 Oracle Service Bus

- The old metric *OSB Service Metrics* appears on the *All Metrics* page to show historical data. However, there is no further collection for this metric.
- The new metric *OSB Service Metrics* has now been divided into the following metrics:
 - *OSB Proxy Service Metrics* that appears under the target component type **OSB Proxy Service**.
 - *OSB Business Service Metrics* that appears under the target component type **OSB Business Service**.

B.4 Oracle WebLogic Server

- The following configuration metrics are collected for the J2EE Application target, and not for the Oracle WebLogic Server target.
 - *General*
 - *Web Services*
 - *Web Service Ports*
 - *JRF Web Services*
 - *JRF Web Services Ports*
 - *JRF Web Services Operations*
 - *JRF Web Services Policy References*
 - *Web Modules*
 - *EJB Modules*
- The following configuration metrics are available for Oracle WebLogic Server version 7, 8, and 9 and higher:
 - *General*
 - *Web Modules*
 - *EJB Modules*
- The following configuration metrics are available for Oracle WebLogic Server version 9 and higher:
 - *Web Services*
 - *Web Service Ports*

- The configuration metric *JDBC Datasource* is now available for all Oracle WebLogic Server targets.
- The data for JDBC Multi Datasource was earlier collected by the metric *JDBC Datasource*. Now the data is collected by the metric *JDBC Multi Datasource*.
- The data for JDBC Connection Pool was earlier collected by the metric *JDBC Connection Pool*. However, this metric is no longer available. All the data collected by that metric has now been moved to the metric *JDBC Datasource*.

These are configuration metrics, and therefore, they do not appear on the *All Metrics* page. Instead, they appear on the *Last Collected* page of the J2EE application.

B.5 JBoss Application Server

In the earlier releases of Enterprise Manager, for monitoring JBoss Application Server, the Management Agent required some JAR files listed in the following file of the agent home:

```
$<AGENT_HOME>/sysman/config/classpath.lst
```

This file was populated during discovery, and the Management Agent had to restart to honor the JAR files location and append to its classpath.

In Enterprise Manager Cloud Control, the `classpath.lst` file is not used because there is a dynamic classloader that loads the classes specific to the target after discovery. So the Management Agent need not restart.

There is a new target instance property `Library Path` that is added to the target metadata. This property is needed by the monitoring logic to differentiate between the case of local and remote monitoring (target monitored by a local or remote agent).

In the case of local monitoring, this property is null.

In the case of remote monitoring, this property is set to the library path location you provide during discovery, which contains the JAR files required for discovering and monitoring JBoss.

During upgrade, ignore this error.

After upgrade, the monitored target status shows as down and no metrics are collected. So set the `Library path` instance property on the Monitoring Configuration page of the target. Set it to the JAR files location.

B.6 Siebel Enterprise

All the metrics available for Siebel Enterprise target have been moved to Siebel Gateway target in Enterprise Manager Cloud Control. As a result, to view the ECM metrics, access the Siebel Gateway target.

B.7 Siebel Server

In the earlier releases of Enterprise Manager, for SARM reports, even log, server process control, and workflow processes, you were required to set only the preferred credentials of the hosts on which Siebel Server and Siebel Gateway Server were running. However, in Enterprise Manager Cloud Control, for these features, you must set several other credentials, besides the host credentials. This section describes the different credentials you must set for various Siebel target types.

This section covers the following:

- [Setting Preferred Credentials for Siebel Server](#)
- [Setting Preferred Credentials for Siebel Gateway Server](#)
- [Setting Preferred Credentials for Siebel Database Repository](#)

B.7.1 Setting Preferred Credentials for Siebel Server

For Siebel Server, set the following credentials:

Host Preferred Credentials	To do so, in Cloud Control, from the Setup menu, select Security , and then, click Preferred Credentials . On the Preferred Credentials page, select Host and click Manage Preferred Credentials . On the Host Preferred Credentials page, set the operating system credentials of the host on which the Siebel Server is running.
Host Credentials for Siebel Server	To do so, in Cloud Control, from the Setup menu, select Security , and then, click Preferred Credentials . On the Preferred Credentials page, select Siebel Server and click Manage Preferred Credentials . On the Siebel Server Preferred Credentials page, in the Target Preferred Credentials section, select the credential set Host Credentials , and click Set to set the operating system credentials of the host on which the Siebel Server is running.
Server Manager Credentials for Siebel Server	To do so, in Cloud Control, from the Setup menu, select Security , and then, click Preferred Credentials . On the Preferred Credentials page, select Siebel Server and click Manage Preferred Credentials . On the Siebel Server Preferred Credentials page, in the Target Preferred Credentials section, select the credential set Server Manager Credentials , and click Set to set the server manager credentials.

B.7.2 Setting Preferred Credentials for Siebel Gateway Server

For Siebel Gateway Server, set the following credentials:

Host Preferred Credentials	To do so, in Cloud Control, from the Setup menu, select Security , and then, click Preferred Credentials . On the Preferred Credentials page, select Host and click Manage Preferred Credentials . On the Host Preferred Credentials page, set the operating system credentials of the host on which the Siebel Gateway Server is running.
Host Credentials for Siebel Gateway Server	To do so, in Cloud Control, from the Setup menu, select Security , and then, click Preferred Credentials . On the Preferred Credentials page, select Siebel Gateway Server and click Manage Preferred Credentials . On the Siebel Gateway Server Preferred Credentials page, in the Target Preferred Credentials section, select the credential set Host Credentials , and click Set to set the operating system credentials of the host on which the Siebel Gateway Server is running.
Server Manager Credentials for Siebel Gateway Server	To do so, in Cloud Control, from the Setup menu, select Security , and then, click Preferred Credentials . On the Preferred Credentials page, select Siebel Gateway Server and click Manage Preferred Credentials . On the Siebel Gateway Server Preferred Credentials page, in the Target Preferred Credentials section, select the credential set Manage Preferred Credentials , and click Set to set the server manager credentials.

B.7.3 Setting Preferred Credentials for Siebel Database Repository

For Siebel Database Repository, set the Siebel DBStore Credentials.

To do so, in Cloud Control, from the **Setup** menu, select **Security**, and then, click **Preferred Credentials**. On the Preferred Credentials page, select **Siebel Database Repository** and click **Manage Preferred Credentials**. On the Siebel Database

Repository Preferred Credentials page, in the Target Preferred Credentials section, select the credential set **Siebel DBStore Credentials**, and click **Set** to set the credentials.

Identifying Jobs That Will Not Run in the Enterprise Manager System

This appendix describes how you can identify the jobs that will not run in the existing Enterprise Manager system and in the upgraded Enterprise Manager system.

- [Identifying Jobs That Will Not Run in the New, Upgraded Enterprise Manager System](#)
- [Identifying Jobs That Will Not Run in the Existing Enterprise Manager System](#)

C.1 Identifying Jobs That Will Not Run in the New, Upgraded Enterprise Manager System

To identify the jobs that will not run in Enterprise Manager Cloud Control, run this SQL query in Enterprise Manager Cloud Control:

```

SET TRIMSPOOL ON
SET VERIFY OFF
SET LINESIZE 80
SET PAGESIZE 500

PROMPT =====
PROMPT Valid on "new" 12.1 EM
PROMPT =====
PROMPT List jobs that will not be run on either system
PROMPT due to a partially migrated target list
PROMPT =====

WITH
-- list of migrated targets
migrated_targets AS
(
SELECT  target_guid
FROM    EM_CURRENT_AVAILABILITY
WHERE   current_status      = 4 -- G_STATUS_UNREACHABLE
AND     current_sub_status = 1 -- G_SUB_STATUS_UNMIGRATED
),
-- list of job related migrated targets
migrate_job_targets AS
(
SELECT  job_id, execution_id, target_guid
FROM    MGMT$JOB_EXECUTION_HISTORY JOIN
        migrated_targets          USING(target_guid)

```

```

WHERE     STATE_CYCLE NOT IN ('FINISHED', 'RUNNING')
),
-- list of jobs against the migrate job targets
effectuated_jobs AS
(
SELECT  count(1) migrated_target_count, job_id, execution_id
FROM    migrate_job_targets
GROUP BY job_id, execution_id
),
-- list of jobs with some unmigrated targets and some migrate targets
partly_migrated_jobs AS
(
SELECT  je.job_id,
        je.execution_id,
        je.job_name,
        je.job_owner,
        je.job_type,
        je.target_name,
        je.target_type,
        je.target_guid
FROM    MGMT$JOB_EXECUTION_HISTORY je,
        effectuated_jobs            ej
WHERE   je.job_id      = ej.job_id
AND     je.execution_id = ej.execution_id
AND     target_guid    NOT IN
        ( SELECT target_guid
          FROM  migrate_job_targets
        )
)
-- list jobs, targets and agents
SELECT  job_name, target_name, target_type
FROM    partly_migrated_jobs
ORDER BY job_name, target_type, target_name;

/*
Could change the last select to
SELECT DISTINCT job_name, job_owner
or
SELECT DISTINCT target_guid

to get the distinct list of jobs or target guids.

or
SELECT DISTINCT emd_url
FROM  partly_migrated_jobs JOIN
      MGMT_TARGETS          USING (target_guid)

to get the distinct list of agents
*/

```

C.2 Identifying Jobs That Will Not Run in the Existing Enterprise Manager System

To identify jobs that will not run in the old, existing Enterprise Manager system, run this SQL query in the old Enterprise Manager system:

```

SET TRIMSPOOL ON
SET VERIFY OFF

```

```

SET LINESIZE 80
SET PAGESIZE 500

PROMPT =====
PROMPT Valid on "original" EM
PROMPT =====
PROMPT List jobs that will not be run on either system
PROMPT due to a partially migrated target list
PROMPT =====
PROMPT Enter a quoted, comma separated list of agent guids about to be
migrated
PROMPT OR any quoted character to list currently stuck jobs
PROMPT =====

WITH
-- list of targets the user is about to migrate
migrating_targets AS
(
SELECT  target_name, target_type, target_guid
FROM    MGMT_TARGETS t
WHERE   t.emd_url IN ( SELECT emd_url
                       FROM    MGMT_TARGETS
                       WHERE   target_guid IN (&p_agent_guid_list)
                       AND     target_type = 'oracle_emd')

--MGMT_GLOBAL.G_AGENT
_TARGET_TYPE )
),
-- list of already migrated targets
migrated_targets AS
(
SELECT  target_name, target_type, target_guid
FROM    PRE_UPGC_TGT_SW
WHERE   STATUS = 'AVAILABLE'
-- NOTE: neither system will monitor targets <> 'AVAILABLE'
--       How to treat them here?
--       For now, treat them as unmigrated
AND     emd_url IN ( SELECT emd_url
                     FROM    PRE_UPGC_AGT_STAT_MGMT JOIN
                           MGMT_TARGETS             USING(target_guid)
                     WHERE   SWITCH_STATUS='STATUS_SUCCESS'
                           OR     SWITCH_STATUS='STATUS_IN_PROGRESS')
),
-- list of job related targets (either migrating or already migrated)
migrate_job_targets AS
(
SELECT  -- use DISTINCT to cover target overlap case
DISTINCT job_id, execution_id, target_guid
FROM    MGMT$JOB_EXECUTION_HISTORY JOIN
        ( SELECT target_guid FROM migrating_targets
          UNION ALL
          SELECT target_guid FROM migrated_targets
        ) USING(target_guid)
WHERE   status NOT IN ('Error',
                       'Failed',
                       'Succeeded',
                       'Skipped',
                       'Stopped')
),
-- list of jobs against the migrate job targets

```

```

effectuated_jobs AS
(
SELECT count(1) migrated_target_count, job_id, execution_id
FROM   migrate_job_targets
GROUP BY job_id, execution_id
),
-- list of jobs with some unmigrated targets and some migrate targets
partly_migrated_jobs AS
(
SELECT je.job_id,
       je.execution_id,
       je.job_name,
       je.job_owner,
       je.job_type,
       je.target_name,
       je.target_type,
       je.target_guid
FROM   MGMT$JOB_EXECUTION_HISTORY je,
       effectuated_jobs            ej
WHERE  je.job_id      = ej.job_id
AND    je.execution_id = ej.execution_id
AND    target_guid    NOT IN
      ( SELECT target_guid
        FROM   migrate_job_targets
        )
)
),
-- list of job related targets (either migrating or already migrated)
migrate_job_targets AS
(
SELECT -- use DISTINCT to cover target overlap case
DISTINCT job_id, execution_id, target_guid
FROM     MGMT$JOB_EXECUTION_HISTORY JOIN
      ( SELECT target_guid FROM migrating_targets
        UNION ALL
        SELECT target_guid FROM migrated_targets
      ) USING(target_guid)
WHERE    status NOT IN ('Error',
                       'Failed',
                       'Succeeded',
                       'Skipped',
                       'Stopped')
),
-- list of jobs against the migrate job targets
effectuated_jobs AS
(
SELECT count(1) migrated_target_count, job_id, execution_id
FROM   migrate_job_targets
GROUP BY job_id, execution_id
),
-- list of jobs with some unmigrated targets and some migrate targets
partly_migrated_jobs AS
(
SELECT je.job_id,
       je.execution_id,
       je.job_name,
       je.job_owner,
       je.job_type,
       je.target_name,
       je.target_type,

```

```

        je.target_guid
FROM    MGMT$JOB_EXECUTION_HISTORY je,
        effected_jobs            ej
WHERE   je.job_id                = ej.job_id
AND     je.execution_id          = ej.execution_id
AND     target_guid              NOT IN
        ( SELECT target_guid
          FROM   migrate_job_targets
        )
)
-- list jobs, targets and agents
SELECT job_name, target_name, target_type
FROM    partly_migrated_jobs
ORDER BY job_name, target_type, target_name;

/*
Could change the last select to
SELECT DISTINCT job_name, job_owner
or
SELECT DISTINCT target_guid

to get the distinct list of jobs or target guids.

or
SELECT DISTINCT emd_url
FROM    partly_migrated_jobs JOIN
        MGMT_TARGETS            USING (target_guid)

to get the distinct list of agents
*/

```


D

Meeting Prerequisites for Installing Oracle Management Agent

Table D-1 lists the prerequisites you must meet before installing Oracle Management Agent (Management Agent).

Table D-1 Prerequisites for Upgrading Oracle Management Agent

Requirement	Description
Hardware Requirements	Ensure that you meet the hard disk space and physical memory requirements. For more information, see the chapter on hardware requirements in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i> .
Operating System Requirements	Ensure that you install Enterprise Manager Cloud Control only on certified operating systems as mentioned in the Enterprise Manager Certification Matrix available on <i>My Oracle Support</i> . To access this matrix, follow these steps: <ol style="list-style-type: none">1. Log in to <i>My Oracle Support</i>, and click the Certifications tab.2. On the Certifications page, in the Certification Search region, from the Product list, select Enterprise Manager Cloud Control.3. From the Release list, select 12.1.0.1.0, and click Search.
Package Requirements	Ensure that you install all the operating system-specific packages. For more information, see the chapter on package requirements in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i> .
User and Operating System Group Requirement	Ensure that the destination host where you want to install the Management Agent has the appropriate users and operating system groups created. For more information, see the chapter on creating operating system groups and users in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i> .
Destination Host Requirements	Ensure that the destination hosts are accessible from the host where the <i>Enterprise Manager 12c Upgrade Console</i> is being used.
Permission Requirements	<ul style="list-style-type: none">■ Ensure that the installation base directory you specify is empty and has <i>write</i> permission.■ Ensure that the instance directory is empty and has <i>write</i> permission.

Table D-1 (Cont.) Prerequisites for Upgrading Oracle Management Agent

Requirement	Description
Path Validation Requirements	Validate the path to all command locations. For more information, see the appendix on validating command locations in the <i>Oracle Enterprise Manager Cloud Control Basic Installation Guide</i> .
Temporary Directory Space Requirements	<p>Ensure that you allocate 400 MB of space for a temporary directory where the executables can be copied.</p> <p>By default, the temporary directory location set to the environment variable <code>TMP</code> or <code>TEMP</code> is honored. If both are set, then <code>TEMP</code> is honored. If none of them are set, then the following default values are honored: <code>/tmp</code> on UNIX hosts and <code>c:\Temp</code> on Microsoft Windows hosts.</p>
Installing User Requirements	<ul style="list-style-type: none"> ■ If the central inventory owner and the user installing the Management Agent are different, then ensure that they are part of the same group. ■ Also ensure that the inventory owner and the group to which the owner belongs have <i>read</i> and <i>write</i> permissions on the inventory directory. <p>For example, if the inventory owner is <i>abc</i> and the user installing the Management Agent is <i>xyz</i>, then ensure that <i>abc</i> and <i>xyz</i> belong to the same group, and they have <i>read</i> and <i>write</i> access to the inventory.</p>
Central Inventory (oraInventory) Requirements	<ul style="list-style-type: none"> ■ Ensure that you allocate 100 MB of space for the Central Inventory. ■ Ensure that the Oracle Inventory (<code>oraInventory</code>) is not in a shared location. When you use the <code>/etc/oraInst.loc</code> file, ensure that the inventory location specified there is not pointing to a shared location. If it is, change it to a non-shared location by following the instructions outlined in <i>My Oracle Support</i> note 1092645.1. ■ Ensure that you have <i>read</i>, <i>write</i>, and <i>execute</i> permissions on <code>oraInventory</code> on all remote hosts. If you do not have these permissions on the default inventory (typically at <code>/etc/oraInst.loc</code>) on any remote host, then ensure that you specify the path to an alternative inventory location by using one of the following options in the Additional Parameters field of the Add Host Targets Wizard: <ul style="list-style-type: none"> <code>INVENTORY_LOCATION=<absolute_path_to_inventory_directory></code> <code>-invPtrLoc <absolute_path_to_oraInst.loc></code>
Default SSH Port Requirements	<p>Ensure that the SSH daemon is running on the default port (that is, 22) on all the destination hosts. To verify the port, run the following command.</p> <pre>netstat -anp grep <port_no></pre> <p>If the port is a non-default port, that is, any port other than 22, then update the <code>SSH_PORT</code> property in the following file that is present in the OMS home:</p> <pre>\$<OMS_HOME>/oui/prov/resources/Paths.properties</pre>

Table D-1 (Cont.) Prerequisites for Upgrading Oracle Management Agent

Requirement	Description
Ping Requirements	<p>If a firewall configured in your environment does not allow any ping traffic, then ensure that you do the following:</p> <ol style="list-style-type: none"> 1. Access the following file from the OMS home: For Linux Platforms: <code>\$<OMS_HOME>/oui/prov/resources/sPaths.properties</code> For Other Platforms: <code>\$<OMS_HOME>/oui/prov/resources/ssPaths_<platform>.properties</code> For example, <code>ssPaths_aix.properties</code> if the OMS is on AIX platform. 2. Change <code>PING_PATH=/bin/ping</code> to <code>PING_PATH=/bin/true</code>.
PATH Environment Variable Requirements	<p>On the destination host, ensure the following:</p> <ul style="list-style-type: none"> ■ (For Microsoft Windows) Ensure that the Cygwin software location appears before other software locations in the <code>PATH</code> environment variable. After making it the first entry, restart the SSH daemon (<code>sshd</code>) on both the hosts. ■ (For UNIX) Ensure that the SCP binaries (for example, <code>/usr/local/bin/scp</code>) are in the <code>PATH</code> environment variable.

Updating Server Load Balancer Configuration Settings

If you have a Server Load Balancer (SLB) configured, make the changes described in [Table E-1](#) to your monitors

Table E-1 SLB-Specific Changes to Monitors

Monitor Name	Configuration					Associated With
	Type	Interval	Timeout	Send String	Receive String	
mon_gcsu1159	https	60	181	GET /empbs/upload	Http Receiver Servlet active!	HostA:1159 HostB:1159
mon_gcar4889	http	60	181	GET /empbs/genwallet	GenWallet Servlet activated	HostA:4889 HostB:4889
mon_gcsc7799	https	5	16	GET /em/console/home HTTP/1.0\n	/em/login.jsp	HostA:7799 HostB:7788
mon_gcuc7788 (optional)	https	5	16	GET /em/console/home HTTP/1.0\n	/em/login.jsp	HostA:7788 HostB:7788

If you have SSO configured, then use the alternate definitions described in [Table E-2](#) for the mon_gcsc7799 and mon_gcuc7788 monitors.

Table E-2 SLB-Specific Changes to Monitors with SSO Configured

Monitor Name	Configuration					Associated With
	Type	Interval	Timeout	Send String	Receive String	
mon_gcsc7799	https	5	16	GET /empbs/genwallet	GenWallet Servlet activated	HostA:7799 HostB:7788
mon_gcuc7788 (optional)	https	5	16	GET /empbs/genwallet	GenWallet Servlet activated	HostA:7788 HostB:7788

Setting Preferred Credentials Using EMCLI

When you provide the agent credentials, you can choose to enter the preferred credentials registered with the Enterprise Manager system. However, ensure that the credentials were registered using EMCLI.

- To register the credentials as preferred credentials for one host at a time, run the following command on the host where the Management Agent is running:

```
emcli set_credential -target_type=host -target_name="<host_name>" -credential_set=OHCreds -column="OHUsername:<em_job_user>;OHPassword:<em_job_pwd>" -oracle_homes="<agent_home>"
```

For example,

```
emcli set_credential -target_type=host -target_name="example.com" -credential_set=OHCreds -column="OHUsername:myuser;OHPassword:2bornot2b" -oracle_homes="/home/john/programs/EM/agent10g"
```

- To register the credentials as default preferred credentials for all hosts at a time, run the following command on one of the hosts where the Management Agent is running. Ensure that the user is a shared user on all the hosts.

```
emcli set_credential -target_type=host -credential_set=OHCreds -column="OHUsername:<em_job_user>;OHPassword:<em_job_pwd>" -oracle_homes="<agent_home>"
```

For example,

```
emcli set_credential -target_type=host -credential_set=OHCreds -column="OHUsername:myuser;OHPassword:2bornot2b"
```

Note: To run these commands, you must have the EMCLI Client installed on the hosts. If you do not have EMCLI, install one following the instructions outlined in *Oracle Enterprise Manager Command Line Interface Guide*.

Searching and Adding Oracle Management Agents

To search and add Oracle Management Agents (Management Agent) on the Deploy and Configure Agents page, Generate Health Report of Deployed Agents page, and on the Switch Agents page, follow these steps:

- To search Management Agents, select the platform and the version of the Management Agents you are searching for, from the **Platform** and **Version** lists, respectively. Then, click **Search**.

Alternatively, if you know the name of the Management Agent, then enter the name in **Agent**, and click **Search**. If you have created a logical group of Management Agents in Enterprise Manager Grid Control, and if you want to list the Management Agents of that group, then from the **Group** list, select the name of that group, and click **Search**.

- The search results in a list of Management Agents discovered in your environment. If you do not want to deploy the software now for some of the Management Agents, then select those Management Agents and click **Remove**.
- In case the search result does not list the Management Agents you are searching for, then click **Add** and manually add the Management Agents of your choice.
- The Management Agent you have added might be part of multiple groups (an Enterprise Manager group), systems (an Enterprise Manager system), or clusters of Management Agents, or it might be associated with multiple shared Management Agents.

In such cases, if you want to select and add the Management Agents of all the groups and clusters, and also the associated shared Management Agents, then click **Add Related Agents**.

Note: If you are adding a *Shared Agent*, then ensure that you add the *Master Agent* to which it communicates, and all the *Shared Agents* that communicate with this *Master Agent*.

Securing Oracle Management Agents After Backing Up Oracle Management Repository

Before you deploy and configure Oracle Management Agents 12c (Management Agent) as described in [Chapter 11](#), you must ensure that the old Management Agents remain in the same mode as they were before the Management Repository was backed up. In other words, if your old Management Agents were running in secure (or unsecure) mode before the Management Repository was backed up, then they must continue to run in the same mode while you deploy and configure the new Management Agents for them.

Do not resecure the Management Agents after backing up the Management Repository. If you do so, the ping test might fail while performing the healthcheck because of a mismatch between the configuration stored in the repository and the actual configuration of the Management Agent. You will see the following `KEY_MISMATCH` error in the `gcagent.log` file.

```
gcagent.log:2011-09-28 05:41:46,192 [82:B5BF5C12:GC.Executor.1 (Ping OMS)] WARN - Received response status KEY_MISMATCH
gcagent.log:2011-09-28 05:42:16,231 [89:D485F18E:GC.Executor.5 (Ping OMS)] WARN - Received response status KEY_MISMATCH
gcagent.log:2011-09-28 05:42:29,232 [1:3305B9] WARN - Received response status KEY_MISMATCH
```

If you still want to resecure the Management Agents for some reason, then follow these steps:

1. Disable the health check by running the following SQL query against the old Management Repository.

```
BEGIN PRE_UPG_UTL.set_param('bypass_hc', '1'); END;
/
commit;
```

2. Switch over the Management Agent as described in [Chapter 14](#).
3. Secure the new Management Agents.

```
$(AGENT_INSTANCE_DIR)/bin/emctl secure agent
```

4. Start the new Management Agents.

```
$(AGENT_INSTANCE_DIR)/bin/emctl start agent
```

5. Enable the health check.

```
BEGIN PRE_UPG_UTL.set_param('bypass_hc', '0'); END;
/
commit;
```



Numerics

- 1-system upgrade approach
 - default ports assigned, 3-4
 - in graphical mode, 16-1
 - in silent mode, 17-1
 - installing software-only
 - in graphical mode, 18-1
 - in silent mode, 19-1
 - overview, 2-1
 - process, 4-1, 6-1
 - using Oracle Software Library, 3-10
 - 1-system upgrade approach on a different host
 - in graphical mode, 20-1
 - overview, 2-2, 3-2
 - using Oracle Software Library, 3-10
 - 2-system upgrade approach
 - default ports assigned, 3-4
 - in graphical mode, 16-9
 - in silent mode, 17-7
 - installing software-only
 - in silent mode, 19-9
 - process, 5-1
- ## A
-
- accrued data, 27-2
 - accrued data migration, 27-1
 - accrued data migration jobs
 - migrating ECM history data, 27-2
 - overview, 27-1
 - signing off, 30-1
 - tracking, 27-2
 - alerts, 3-7
 - closed alerts, 3-7
 - creating incidents and events, 3-8
 - migration methods, 3-7
 - open alerts
 - creating incidents and events, 3-7
 - migration, 3-7
 - allroot.sh script, 16-7
 - Application Dependency and Performance, 4-4, 5-2, 6-4, 6-5
 - architecture, 1-3

C

- central inventory, 10-1, D-2
- centralized monitoring, 1-1
- configuration assistants, 2-10, 2-12
- connectors, 3-10
- console, 1-5
- critical data migration, 26-1

D

- data format migration, 26-1
- database
 - backing up database, 5-4
 - backing up with DBCA, 5-4
 - providing repository backup details, 15-1
- database upgrade, 3-2
- deferred data migration jobs
 - deferred data migration, 26-1
 - overview, 26-1
 - tracking, 26-2
- deploy operations, 2-8
- deployment procedures, 2-3, 4-3, 5-2
- diff reports
 - generating and viewing, 28-1
 - overview, 28-1
- discovering targets, 3-6
 - automatic, 3-6
 - manual, 3-6
- downtime
 - minimum or zero downtime, 2-2
 - reasonable, 2-2
 - reasonable downtime, 2-2

E

- EM_UPLOAD_HTTP_PORT parameter, 8-2
- EM_UPLOAD_HTTPS_PORT parameter, 8-2
- EMCLI, F-1
- EMCLI clients, 3-11
- emgc.properties file, 8-2
- emkey, 4-4, 5-3, 5-5, 6-4
- Enterprise Manager Cloud Control
 - supported upgrade paths, 3-1
 - accessing upgrade console, 2-5

- architecture, 1-2, 1-3
- console, 1-5
- core components, 1-2
- installation wizard, 2-6
- overview, 1-1
- postupgrade console, 2-7
- postupgrade steps, 25-1
- preupgrade console, 2-4
- supported platforms for upgrade, 3-2
- upgrade approaches, 2-1
- upgrade scope, 3-2
- upgrade utilities, 2-4
- upgrading multi-OMS environment, 21-1

Enterprise Manager Cloud Control Installation Wizard, 2-6

enterprise rulesets, A-2

events, 3-7, A-1

- overview, A-1

F

- failed jobs, 3-9
- firewall settings, 2-3, 3-4

G

- gc_inst directory, 2-10, 3-2
- GCDomain, 2-9

H

- health report, 12-1
 - generating, 12-1
 - signing off, 13-1
 - verifying, 13-1

I

- identifying host for upgrade, 8-1
- inactive targets, 29-1
- incident rule sets
 - deleting rule sets, 25-3
- incident rules, 31-1
 - deleting, 31-5
 - overview, 31-1
 - updating for moved metrics, 31-3
 - updating for renamed metrics, 31-4
- Incident rulesets, A-1
- incident rulesets, 3-7, 31-1, A-1
 - accessing, A-2
 - classification, A-2
 - migrating notification rules, A-3
- incidents, A-1
 - overview, A-1
- incidents and events, 3-7
- installation base directory, 11-3, D-1
- instance directory, D-1
- inventory.xml file, 10-1, 10-2, 10-3

J

- Java Development Kit, 2-9
 - default version, 2-11, 2-13
 - default version installed, 3-2
 - manual download, 3-3
- JDK, 2-9
- jobs
 - 1-system upgrade approach, 3-8
 - 2-system upgrade approach, 3-8
 - aborted jobs, 3-9
 - jobs on multiple targets, 3-10
 - management, 3-8
 - repeating jobs, 2-4, 3-9
 - running, 2-3
 - scheduled jobs, 2-3, 3-8
 - suspended jobs, 3-9
- JROCKIT, 3-3
- JVM Diagnostics, 4-4, 5-2, 6-4, 6-5

L

- lifecycle management, 1-1
- linux patching, 25-4
- lockd account
 - using locked account, 11-4
- locked account
 - power broker, 11-4
 - SUDO, 11-4

M

- managed hosts, 1-4
- managed server, 2-9
- Management Agent, 1-4
- Management Repository, 1-4
- management repository
 - creating link to upgraded repository, 22-1
- managing software, 9-1
- master agents, 11-3
- metric changes, B-1
- metric collection errors, 12-3, 25-3
- metrics
 - changes, 31-1
 - collecting metrics, 3-11
 - decommissioned, 31-3
 - moved, 31-2
 - renamed, 31-2
 - renamed metrics, 3-11
 - retained, 31-2
 - thresholds, 3-11
- migration activity, 26-1, 27-1
- minimal monitoring loss, 2-1
- missing agent or plug-in software, 10-4
- monitoring targets, 3-6
- multi-OMS environment, 8-1, 21-1

N

- near-zero downtime, 2-1
- NFS-mounted drive, 3-2

- node manager, 2-9
- not supported, 10-3, 10-4
- notification, 3-7
- notification methods, A-4
- notification rules, 3-7, 31-1, A-1
- notifications, A-1

O

- obsolete targets, 25-2
- OCM scheduler, 25-1
- OMS, 1-4
- operating system groups, D-1
- operating system users, D-1
- operation name, 11-2
- Oracle HTTP Server, 3-2
- Oracle JRF, 2-13
- Oracle Management Agent, 1-4
 - agent upgradability, 9-1
 - analyzing environment, 10-1
 - checking agent upgradability status, 10-3
 - configuring, 11-1
 - deploying, 11-1
 - generating health report, 12-1
 - manual download, 9-2
 - prerequisites, D-1
 - problematic agents, 10-4
 - reconfiguring, 11-6
 - target upgradability, 9-1
 - upgradable, 10-3
 - upgrade status, 24-1
 - upgrading
 - installing plug-ins, 3-4
 - with invalid inventory, 10-2
 - with valid inventory, 10-1
- Oracle Management Plug-Ins, 1-4
- Oracle Management Repository, 1-4
 - upgrading
 - in graphical mode, 16-1
 - in silent mode, 17-1
- Oracle Management Service, 1-4
 - installing software-only
 - in graphical mode, 18-1
 - in silent mode, 19-1
 - stopping OMSes, 16-4
 - upgrading
 - in graphical mode, 16-1
 - in silent mode, 17-1
 - installing plug-ins, 3-5
- Oracle Software Library, 3-10
 - backing up software library, 5-3
 - NFS-mounted drive accessible, 6-5
 - reconfigure software library, 5-6
 - using the library
 - 1-system upgrade approach, 3-10
 - 1-system upgrade approach on a different host, 3-10
 - 2-system upgrade approach, 3-10
- Oracle Software Library Reconfigure Locations page, 23-2

- Oracle Web Tier, 2-9, 2-13
- Oracle WebLogic domain, 2-9
- Oracle WebLogic Server, 2-11, 2-13
 - default version installed, 2-9, 3-2
 - manual installation, 3-3
 - typical installation, 3-3
- oracle_common directory, 2-9, 2-11, 2-13
- ORACLE_COMMON property, 3-3
- Oracle_WT directory, 2-9, 2-11, 2-13
- oraInst.loc file, 10-3
- out-of-place upgrade, 3-2

P

- packages, D-1
- pie charts, 9-1
- ping, 13-1, D-3
- ping test, 11-1, 13-1
- pluggable entities, 1-4
- plug-ins, 1-4
 - downloading required plug-ins, 3-5, 9-2
 - identifying required plug-ins, 3-4
 - installed by default, 2-9, 2-11, 2-13
 - installing, 3-4
 - installing while upgrading Management Agent, 3-4
 - installing while upgrading OMS, 3-5
 - mandatory plug-ins, 1-4, 1-5
 - manual download, 16-7
 - manual installation, 16-8
 - overview, 1-4
- ports
 - default ports assigned, 3-4
 - HTTP upload ports, 8-2
 - HTTPs upload ports, 8-2
 - reusing existing ports, 3-4
 - secure, 8-1, 8-2
 - unsecure, 8-1, 8-2
- Post Upgrade Reconfiguration, 23-1
- post-config options, 11-5
- post-upgrade activity, 27-1
- postupgrade console, 2-7
- postupgrade steps
 - disabling incident rule sets, 25-3
 - enabling linux patching, 25-4
 - general, 25-1
 - resolving metric collection errors, 25-3
 - stopping OCM scheduler, 25-1
- postupgrade tasks, 25-1
- power broker, 11-4
- pre-deploy options, 11-4
- preferred credentials, 11-4, F-1
 - default selection, 11-4
 - overriding preferred credentials, 11-4
 - registering
 - as default credentials, F-1
 - as preferred credentials, F-1
 - registering with EMCLI, 11-4
- private cloud, 1-1
- private rulesets, A-2

- problematic agents, 10-5
- process
 - 1-system upgrade approach, 4-1, 6-1
 - 2-system upgrade approach, 5-1
- processes
 - 1-system upgrade, 2-8
 - 1-system upgrade on a different host, 2-13
 - 2-system upgrade, 2-10
- public cloud, 1-1

R

- readiness check, 12-2
- reconfiguration Software Library validation
 - errors, 23-3
- reconfiguring Oracle Software Library, 23-1
 - confirmation step, 23-4
 - validation step, 23-3
- registering, 9-1
- repository backup details, 15-1
- root.sh script, 11-6

S

- secure ports, 8-1
- securing the OMS, 2-12
- server load balancer
 - changes to monitors, E-1
 - changes to monitors with SSO configured, E-1
 - updating configuration, E-1
- server load balancers, 6-4
- shared agents, 11-3
- signing off accrued data migration jobs, 30-1
- skipped jobs, 3-9
- SOA targets, 12-3, 13-3
- software library
 - See Oracle Software Library, 3-10
- software location
 - validating, 9-1
- software updates
 - installing, 16-2, 16-11
 - installing from custom location, 16-11
 - skip installing, 16-2, 16-11
- software-only mode, 18-1
- SSH ports, D-2
- stage location, 9-2
- staticports.ini file, 16-6
- SUDO, 11-4
- supported upgrade paths, 3-1
- suspended on event, 11-6, 12-3
- switch over operations, 2-8
- switchover
 - generating health report, 12-1
 - signing off health report, 13-1
 - switching over, 14-1
 - verifying health report, 13-1
- system upgrade approach
 - using Oracle Software Library, 3-10

T

- target types added, 31-1
- targets
 - checking the upgradability status, 10-4
 - upgradable, 10-4
- temporary directory, D-2
- two-system upgrade
 - reconfiguring Oracle Software Library, 23-1
 - two-system reconfiguration, 23-3

U

- unmanaged hosts, 1-4
- unsecure upload ports, 8-1
- upgrade
 - 1-system upgrade in graphical mode, 16-1
 - 1-system upgrade in silent mode, 17-1
 - 1-system upgrade on a different host in graphical mode, 20-1
 - 2-system upgrade in graphical mode, 16-9
 - 2-system upgrade in silent mode, 17-7
 - agent upgrade status, 24-1
 - installing software-only
 - 1-system upgrade in graphical mode, 18-1
 - 1-system upgrade in silent mode, 19-1
 - 2-system upgrade in graphical mode, 18-9
 - 2-system upgrade in silent mode, 19-9
- upgrade approaches, 2-1
 - 1-system upgrade approach, 2-1
 - 1-system upgrade approach on a different host, 2-2
 - 1-system upgrade process on a different host, 2-13
 - 2-system upgrade approach, 2-1
 - 2-system upgrade process, 2-10
 - differences, 2-2
 - overview, 2-1
- upgrade console
 - applying patch, 4-1, 5-1, 6-1
- upgrade options, 2-1
- upgrade scope, 3-2
- upgrade utilities, 2-4
- upgrade.rsp file, 17-1
- user accounts
 - SYS, 16-4
 - SYSMAN, 16-4

V

- valid inventory, 10-1

W

- with missing agents software, 10-3
- with missing plug-ins, 10-3
- WLS_DOMAIN_NAME option, 16-7
- wls1035_generic.jar file, 3-3